CYBER SECURITY
RESEARCH AND DEVELOPMENT
BROAD AGENCY ANNOUCEMENT (BAA)
BAA 11-02

Published: January 26, 2011

Table of Contents

I. INTRODUCTION.

A. This solicitation is a Broad Agency Announcement (BAA), as contemplated in Federal Acquisition Regulations (FAR) 6.102(d)(2) and 35.016. A formal Request for Proposal (RFP) will not be issued in this matter.

B. Cyber attacks are increasing in frequency and impact. Even though these attacks have not yet had a significant impact on our Nation's critical infrastructures, they have demonstrated that extensive vulnerabilities exist in information systems and networks, with the potential for serious damage. The effects of a successful cyber attack might include: serious consequences for major economic and industrial sectors, threats to infrastructure elements such as electric power, and disruption of the response and communications capabilities of first responders.

C. A critical area of focus for DHS is the development and system prototype demonstration in an operational environment of technologies to protect the nation's cyber infrastructure, including the Internet and other critical infrastructures that depend on computer systems for their mission.

D. The DHS S&T mission is to conduct, for homeland security purposes, research, development, test and evaluation (RDT&E) and timely transition of cyber security capabilities to operational units within DHS, as well as local, state, Federal and operational end users in critical infrastructure. Cyber security is defined in broad terms to encompass the usual attributes of security, as well as reliability, availability, and survivability in the face of adversary attack and accidental fault, while preserving privacy.
DHS S&T invests in programs offering the potential for revolutionary changes in technologies that promote homeland security and accelerate the prototyping and system prototype demonstration in an operational environment of technologies that reduce homeland vulnerabilities. DHS S&T performs these functions in part by awarding procurement contracts, grants, cooperative agreements, or, if authorized by law at time of award, Other Transaction Agreements (OTAs) for research or prototypes to public or private entities, businesses, and federally funded research and development centers and universities. DHS bears the responsibility of helping to secure a substantial portion of our nation's critical infrastructure, including information and telecommunications, transportation, postal and shipping, emergency services and government continuity. However, it does not own or control this infrastructure; according to estimates, the private sector owns and operates 85 percent of the nation's critical infrastructure.

II. GENERAL INFORMATION.

A. **Agency Name:**

Department of Homeland Security
Science & Technology Directorate
Washington, DC 20528

B. **Research Opportunity Title:** Cyber Security Research and Development

C. **Program Name:** Cyber Security

D. **Research Opportunity Number:** BAA 11-02

E. **Response Dates:**

Event	Time Due	Date Due	Registration Location
White Paper Registration Due*	4:30pm EST	February 16, 2011	https://baa2.st.dhs.gov
White Papers Due	4:30pm EST	March 1, 2011	https://baa2.st.dhs.gov
Proposals due (from offerors whose white papers are deemed as being "of particular value")	4:30pm EST	May 26, 2011	https://baa2.st.dhs.gov

*Note: Offerors must register by the white paper registration due date in order to submit a white paper in response to this BAA. Only offerors whose white papers are deemed as being "of particular value" to DHS S&T may submit a proposal in response to this BAA.

F. **Government Representatives:**

1. Science and Technology.

   Douglas Maughan, Ph.D.
   Director
   Cyber Security Division
   Department of Homeland Security
   Homeland Security Advanced Research Projects Agency (HSARPA)
   Science and Technology (S&T) Directorate
   Washington DC, 20528

2. Business.

   Cherita Thomas
   Contracting Officer
   Department of Homeland Security
   Science & Technology Acquisitions
   Washington, DC 20528

G. **Inquiries:**

1. Submit any technical and/or contractual inquiries to this BAA to**:** STCyberSecurityBAA@hq.dhs.gov.

2. For any difficulties with white paper registration, white paper submissions, or proposal submissions using the procedures identified in VIII.A and IX.D contact (703) 480-7676 or dhsbaa@reisys.com.

H. **Catalog of Federal Domestic Assistance (CFDA) Number:** 97.065

I. **Catalog of Federal Domestic Assistance (CFDA) Title:** Homeland Security Advanced Research Projects Agency

III. RESEARCH OPPORTUNITY DESCRIPTON.

A. Goals of DHS Cyber Security Division (CSD). The goals of the DHS Cyber Security Division (CSD) are:

1. To perform research and development (R&D) aimed at improving the security of existing deployed technologies, and to ensure the security of new emerging systems;

2. To develop new and enhanced technologies for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure; and

3. To assist the transfer of these technologies into the national infrastructure as a matter of urgency.

B. To achieve the above goals, BAA 11-02 calls for research and development in fourteen Technical Topic Areas (TTAs). Appendix A provides a detailed description of each of these 14 TTAs.

C. Offerors interested in this opportunity may submit a white paper and, if deemed of particular value, a proposal for one or more of the 14 TTAs in accordance with the procedures outlined herein. Submitted white papers shall identify which one of three Type classifications, described below, aligns with the proposed technology.

1. Type I (New Technologies): Proposals requesting funding for new technologies shall have an applied research phase and a development phase, including technology demonstrations in an operational environment. The emphasis for this type is on research and development, with the technology demonstrations in an operational environment effort included as an option. Proposals may request funding not to exceed $3M for a timeframe not to exceed 36 months, including the option for technology demonstrations in an operational environment.

2. Type II (Prototype Technologies): Proposals requesting funding for more mature prototype technologies shall have a development phase, including technology demonstrations in an operational environment. Proposals may request funding not to exceed $2M for a timeframe not to exceed 24 months.

3. Type III (Mature Technologies): Proposals requesting funding for a mature technology shall consist only of the effort to conduct technology demonstrations in an operational environment. Proposals may request funding not to exceed $750K for a timeframe not to exceed 12 months.

D. The objective of the above identified structure is to support immediate technology transition wherever possible, and to create transition paths for new capabilities from the outset.

IV. TEST AND EVALUATION FACILITIES.

A. Performers in the DHS S&T CSD (Cyber Security Division) technical program will be required to test and evaluate their technologies with respect to system performance goals. Performers may use the facilities of the Cyber Defense Technology Experimental Research (DETER) network, as well as other facilities as appropriate. The DETER testbed provides the necessary infrastructure—networks, tools, and supporting processes—to support national-scale experimentation on emerging security research and advanced development technologies.

B. The DETER testbed was jointly funded by DHS S&T and the National Science Foundation (NSF). It has been open to the research community since March 2004. The project objectives were to build an effective experimental and testing environment, and to develop a corresponding experimental methodology for Internet security issues and defense mechanisms. The testbed is evolving in scope, function, and operational readiness, and should be usable for a number of projects associated with the TTAs.

C. The centerpiece of the experimental environment is a safe (quarantined), but realistic, network testbed. The design of the DETER testbed is based on a mesh of clusters of homogeneous experimental nodes. Each cluster in turn is based upon Utah's Emulab hardware and software, with additions and modifications to provide the security and isolation that is a unique requirement of the DETER testbed. The needs and goals of networking researchers should drive network research testbeds, and the DETER testbed has been designed to meet the particular needs of researchers in network security. Important examples of application areas for the DETER testbed include, but are not limited to, distributed denial-of-service (DDoS) defense, worm propagation and defense, and defense of the network control plane, e.g., routing infrastructure and DNS. In addition to the testbed itself, the DETER testbed is creating a supporting software environment of attack, defense, traffic generation, measurement, and analysis tools.

D. Offerors responding to BAA 11-02 should bear in mind that the design of the DETER testbed is itself an important research and engineering problem. Offerors should not expect a ready-made "turnkey" platform on which their proposed technologies can be immediately tested and evaluated. Rather, CSD performers should expect to become active participants in the community of security researchers that will shape the development of the DETER testbed. Accordingly, offerors should consider the specific test and evaluation requirements of the proposed technical solutions and, if appropriate, include plans for participation in the DETER community. Offerors may propose test and evaluation plans in testbeds other than DETER, showing clearly how the proposed testbed will better serve the CSD program with respect to system performance goals. Not using the DETER testbed facility will not negatively affect a proposal. All proposals are required to include the associated costs for any testing and evaluation, regardless of testbed facility identified.

E. Option to Use DETER as a Secondary Testbed.

1. When the use of DETER is not identified as the testbed for the technology proposed or when testing and evaluation is complete or substantially complete for the technology proposed, the Government will consider, as an option to be exercised at a later date, the award of additional testing using the DETER testbed.

2. This option is meant to provide an additional incentive for performers to engage, leverage, and help strengthen available test and evaluation facilities and services available through DETER.

3. The Government reserves the right to exercise this option and, if exercised, will award:

a. A maximum of $50,000 towards the offeror's proposed costs for utilizing DETER as a secondary testbed. Any costs proposed in excess of $50,000 will be the responsibility of the entity receiving any resultant award; and

b. A maximum of six months of additional time over the timeframe limitations identified in the Type classification descriptions included in paragraph III.C. above.

4. For purposes of evaluation:

a. The offeror's proposed total cost to use DETER as a secondary testbed will not be considered as part of the maximum funding limitation for the Type classification assigned to the technology proposed. However, the proposed costs will be evaluated for reasonableness and completeness in accordance with paragraph X.A.5, Criterion V.

b. The maximum timeframe of six months to complete the testing and evaluation when using DETER as a secondary testbed will not be considered as part of the maximum timeframe identified for the Type classification assigned to the technology proposed. However, the soundness of the technical and managerial approach for completing the

testing and evaluation using DETER will be evaluated in accordance with paragraph X.A.1., Criterion I.

5. Offers who elect to include an option for the Government to award DETER as a secondary testbed shall include the appropriate documentation required herein with any white paper and proposal submissions.

F. More information on the DETER testbed design, implementation, and operational policies and procedures can be found at the main DETER project Web site at: http://www.isi.edu/deter/.

G. Additional information on the testbed operations Web site at: http://www.isi.deterlab.net/.

V. RESEARCH DATASETS.

A. Performers in the DHS S&T CSD technical program will be required to test and evaluate their technologies with respect to system performance goals. Performers are free to provide their own datasets, or they can use those available through the PREDICT repository.

B. In response to the ongoing need for datasets and the problem for the networking and information security research communities, DHS S&T has established the Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) program.

C. The goal of PREDICT is to create a national research and development resource to bridge the gap between the producers of security-relevant network operations data and technology developers and evaluators. Developers and evaluators can employ such data to accelerate the design, production, and evaluation of next-generation, cyber security solutions, including commercial products.

D. PREDICT will acquire, index, and maintain sets of data on Internet traffic from private-sector and academic network operators, and make those datasets available to researchers for studies on cyber security. This data will be provided to cyberdefense researchers to develop new models, technologies, and products that support effective threat assessment and increase cyber security capabilities. One of the most important aspects of the PREDICT repository is the anonymization, where appropriate, of the data to ensure privacy protection for the data provider.

E. More information on the PREDICT repository and its operational policies and procedures can be found at the main PREDICT project Web site: https://www.predict.org.

VI. ELIGIBILITY INFORMATION.

A. BAA 11-02 is open to **ALL** responsible sources. Foreign or foreign-owned offerors are advised that their participation is subject to the foreign disclosure review procedures, applicable export control laws, and other applicable federal laws, regulations, and policies pertaining to foreign entities. It is the intent of research and development contracting to obtain a broad base of the best contractor resources from the scientific and industrial community, to include small businesses and as a result, no portion of BAA 11-02 will be set aside pursuant to FAR Part 19.502-2. Offerors may include (but are not limited to):

1. Single entities or teams from private-sector organizations;

2. Government laboratories;

3. Federally Funded Research & Development Centers (FFRDCs), including Department of Energy national laboratories and centers and academic institutions as long as they are permitted under a sponsoring agreement between the Government and the specific FFRDC;

4. Historically Black Colleges and Universities (HBCU);

5. Minority Institutions (MI);

6. Small & Small Disadvantaged Business concerns, including Women-Owned Small Business concerns, Veteran-Owned Small Business concerns, Service-Disabled Veteran-Owned Small Business concerns, and Historically Underutilized Business Zone (HUBZone) Small Businesses concerns; and

7. Any academic institutions or non-profits organizations not included in the above categories.

B. Any offerors may join others as team members in submitting proposals.

VII. INFORMATION REGARDING RESULTANT AWARDS.

A. **Funding**:

1. Although subject to official fiscal appropriation, it is anticipated that the Cyber Security program will have approximately $40M for award under BAA 11-02.

2. The current Continuing Resolution (CR) is not applicable to this requirement. The CR provides funding for continuing projects or activities that were conducted in FY 2010, and for which appropriations, funds, or other authorities were previously made available. The CR provides this funding at a rate for operations as provided in the applicable appropriations act for FY 2010 and under the authority and conditions provided in that act.

Since the effort to be conducted as a result of BAA 11-02 was programmed in FY10, awards resulting from BAA 11-02 may be made upon selection of successful proposals.

B. **Anticipated Number of Awards:** DHS S&T expects to make one or more awards for each TTA.

C. **Anticipated Award Types:**

1. It is anticipated awards from BAA 11-02 to be in the form of cost reimbursement type contracts. However the Government reserves the right to award grants, cooperative agreements, OTAs (if authorized by law at time of award), or interagency agreements to appropriate parties should the situation warrant.

2. In the event an offeror or subcontractor is a Federally Funded Research and Development Center (FFRDC), Department of Energy National Laboratory, or other Federally funded entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 U.S.C. 1535) or other appropriate authority.

D. **Expected Amounts of Individual Awards:**

1. Type I (New Technologies). Each award resulting from a Type I proposal will not exceed $3 million, excluding the value for the option to use DETER as a secondary test site as described in paragraph IV.E. above.

2. Type II (Prototype Technologies). Each award resulting from a Type II proposal will not exceed $2 million, excluding the value for the option to use DETER as a secondary test site as described in paragraph IV.E. above.

3. Type III (Mature Technologies). Each award resulting from a Type III proposal will not exceed $750K, excluding the value for the option to use DETER as a secondary test site as described in paragraph IV.E. above.

E. **Anticipated Periods of Performance for Individual Awards:**

1. Type I (New Technologies). The period of performance for each award resulting from a Type I proposal will not exceed 36 months, including the system prototype demonstration in an operational environment phase. The 36-month maximum timeframe excludes the six month maximum timeframe identified for the option to use DETER as a secondary test site as described in paragraph IV.E. above.

2. Type II (Prototype Technologies). The period of performance for each award resulting from a Type II proposal will not exceed 24 months, including the system prototype demonstration in an operational environment phase. The 24-month maximum timeframe excludes the six month maximum timeframe identified for the option to use DETER as a secondary test site as described in paragraph IV.E. above.

3. Type III proposals (Mature Technologies). The period of performance for each award resulting from a Type III proposal will not exceed 12 months. The 12-month maximum timeframe excludes the six month maximum timeframe identified for the option to use DETER as a secondary test site as described in paragraph IV.E. above.

VIII. WHITE PAPER REGISTRATION AND SUBMISSION REQUIREMENTS.

A. **White Paper Registration:** White paper submissions will not be accepted from organizations that have not registered by the due date outlined in paragraph II.E. above. Procedures for white paper registration are as follows:

1. To begin the registration process, log on to https://baa2.st.dhs.gov and select *Proposal Submission* link from the side menu. Note users will need their respective company's Tax Identification Number (TIN) or Employee Identification Number (EIN) to complete registration.

2. After logon, click on "Start New Proposal" to initiate a new white paper registration, and fill in the requisite fields, including selecting the specific Technical Topic Area (TTA) (#1-#14) to be addressed by the proposed technology. Note on this page, click on the "register a solicitation". For additional information download the training guide that can be obtained from the upper left hand corner of the FAQs tab.

3. Offerors may register to submit as many white papers for as many TTAs as desired. Each white paper submitted must address a primary TTA. If the proposed technology has any relationship to other TTAs over and above the TTA the white paper will be submitted under, then the white paper should address how the proposed technology relates to these additional TTAs.

4. If submitting multiple white papers, it is NOT necessary to register multiple times. Registration for multiple white papers can be made by using the Start New Proposal button as many times as needed.

B. **White Paper Format:** White papers may include narrative, pictures, figures, tables, and charts in a legible size, and must be accompanied by a one-page quad chart. Format details are:

1. Paper Size: 8.5-by-11-inch paper.

2. Margins: 1 inch.

3. Spacing: Single or double-spaced.

4. Font: Times New Roman, no smaller than 12 point. Text embedded within graphics or tables in the body of the white paper or the quad chart may not be smaller than 10 point.

5. Number of Pages: No more than seven single-sided pages consisting of the following shall be submitted:

a. A cover page;
b. Five pages of technical content; and
c. A one-page quad chart (refer to paragraph VIII.B.8. below for quad chart format).

6. ***WHITE PAPERS EXCEEDING THE ABOVE PAGE LIMIT WILL NOT BE EVALUATED.***

7. Copies: A white paper shall consist of ONE electronic file in portable document format (PDF), readable by IBM-compatible personal computers (PCs). The quad chart must be submitted in the same file as the white paper. The file size must be no more than 10 megabytes (MB). Refer to paragraph VIII.B.8. below for quad chart format.

8. Quad Chart Format: Quad charts will not use any font smaller than 12-point, except in graphics or tables, which may use 10-point fonts, and will be organized as follows:

BAA Number: Cyber Security BAA XX-XX	Offeror Name:
Title: *(Brief/Short Title to Describe Offeror's Proposed Effort)*	Date:

Photograph or artist's concept: *Provide a simple but sufficiently detailed graphic that will convey the main idea of the final capability/use/system prototype demonstration in an operational environment , and its technological methodology.*	Operational Capability: 1. *Performance targets* 2. *Quantify performance for key parameters* 3. *Cost of ownership* 4. *Address how the proposed development addresses the goals in the BAA.*
Proposed Technical Approach: 1. *Explain how it would meet and/or exceed the requirement/goals detailed in the BAA.* 2. *Describe tasks to be performed for base period.* 3. *Describe current status of the proposed technology.* 4. *Describe any actions done to date.* 5. *Describe any related ongoing effort by the offeror.*	Schedule, Cost, Deliverables, & Contact Info: *Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option.* *Deliverables:* *Include all hardware, software and data deliverables.* *Corporate Information:* *You must include Offeror Name, POC full name, address, phone numbers and e-mail.*

9. Proprietary Marking. Offerors are expected to appropriately mark each page of the white paper that contains proprietary information.

C. **White Paper Content:** The Government will evaluate white papers as described herein to determine those submittals deemed as being "of particular value" to DHS S&T. Submittals deemed as being "of particular value" will be invited to submit proposals. White papers shall be succinct and shall include, as a minimum, the following:

1. Cover Page: The cover page shall be labeled "Proposal White Paper", and shall include the following:

a. BAA number, i.e., "BAA 11-02";
b. Title of proposal;
c. Name of offeror's organization and offeror's administrative and technical points of contact, including name, address, telephone and facsimile numbers, and email addresses. If multiple organizations are participating, identify the above information for each organization;
d. Identify whether the offeror (and each organization participating) is a US or foreign owned entity;

e. Type classification as described in paragraph III.C. above (Type I, Type II, or Type III) that aligns with the proposed technology; and

f. The signature and title of an authorized representative of the entity submitting the white paper.

2. Quad Chart: A quad chart shall be included and shall be in the format identified in paragraph VIII.B.8. above.

3. Technical Content: The remaining five pages of the white paper shall consist of the following information:

a. Executive Summary: An executive summary shall be provided containing a concise description of the scientific, technical, engineering, and management approach you propose to address through the TTA, a description of the various features of the proposed technology, and relevant details about how it will meet the requirements of the TTA(s).

b. Utility to Department of Homeland Security: The white paper shall describe the potential of the technology for meeting the desired topic attributes and requirements given in BAA 11-02.

c. Technical Approach:

(1) Provide a description of the basic scientific or technical concepts that comprise the proposed solution to the problem described in the TTA.

(2) Explain what is unique about the proposed solution and what advantages it might afford compared to other approaches that have been taken in this area. Illustrate the particular scientific, technical, or engineering issues that need to be addressed and resolved to demonstrate feasibility.

(3) Describe all required material, such as previously developed technology, test and evaluation facilities (e.g., DETER), or other information which must be provided by the Government to support the proposed work**.** If using a testbed other than DETER, show clearly how the proposed testbed will better serve the CSD program with respect to system performance goals. Not using the DETER testbed facility will not negatively affect an offeror's submission.

d. Personnel and Performer Qualifications and Experience: Briefly describe the offeror's qualifications and experience in similar development efforts. Present the qualifications of the principal technical personnel. Submission shall include the identification of at least two key personnel who, if a resultant award is made, will be subject to any key personnel clauses included in the resultant award. Describe the extent of your team's past experience in working with or developing the technologies comprising your solution. For submissions that include multiple organizations, all organizations must be identified. Include a description of what role each organization will play in the project,

identify appropriate technical personnel for each organization, and each team member's past experience in technical areas related to the white paper.

e. Commercialization Capabilities and Plan: Provide a brief summary of the offeror's capabilities and experience in transitioning similar products to the marketplace, including previous business partnerships that can be leveraged. Describe the commercialization plan or other transition method for getting the technology into widespread use.

f. Costs, Work, and Schedule: Provide a brief summary of the planned work, costs, and schedule required to execute your project, summarized by major task.

D. **White Paper Submissions:**

1. Offerors must submit a white paper in order to be considered for participation in the submission of proposals. White paper submissions will not be accepted from organizations that have not registered by the due date outlined in paragraph II.E. above.

2. Multiple white papers may be submitted in accordance with the terms outlined in paragraph VIII.A. 3 above.

3. The due date for the submission of white papers is no later than 4:30 P.M. (Local Eastern Time) on **March 1, 2011**. White papers **WILL NOT BE ACCEPTED** after the established due date.

4. Procedures for submitting a white paper are as follows:

a. After logon to https://baa2.st.dhs.gov, click on "Start New Proposal" to initiate a new white paper.

b. Input the basic submission information - select BAA 11-02 from the *Solicitation* drop down. Select a topic area from the *Topic* drop down. Input a title and click "Add Proposal to Activity Worksheet". The white paper will be added to your proposal activity worksheet.

c. From the proposal activity worksheet, fill out the requisite fields, upload the white paper files, and then submit. Offerors submitting a white paper will receive confirmation of the submission via e-mail. For additional information download the training guide that can be obtained from the upper left hand corner of the FAQs tab.

5. An offeror's white paper may be revised until the white paper submission deadline outlined in paragraph II.E. above. Failure to submit a white paper will disqualify an offeror from consideration for submitting a proposal.

6. No classified white papers will be accepted.

7. In teaming situations, the lead/prime organization must remain the same on both the white paper and, if selected, the proposal.

IX. PROPOSAL SUBMISSION REQUIREMENTS.

A. **Eligible Proposal Submissions:** Only offerors whose white papers are deemed as being "of particular value" to DHS S&T will be invited to submit proposals. The Government will advise, in writing, those offerors whose white papers are deemed as being "of particular value". For those offerors who submitted multiple white papers, the Government will provide notification regarding whether the white paper is "of particular value" for each individual white paper submitted. ***PROPOSALS WILL NOT BE ACCEPTED FROM ANY OFFERORS OTHER THAN THOSE INVITED TO SUBMIT PROPOSALS***.

B. **Proposal Format:**

1. Proposals will consist of two volumes:

Volume 1 – Technical Proposal
Volume 2 – Cost Proposal

2. For each volume, the following format shall apply.

a. Paper Size: 8.5-by-11-inch paper.

b. Margins: 1 inch.

c. Spacing: Single or double-spaced.

d. Font: Times New Roman, no smaller than 12 point. Text embedded within graphics or tables in the body of the white paper or the quad chart may not be smaller than 10 point.

e. Number of Pages:

(1) Volume 1: No more than 40 single-sided pages. Proposals exceeding the page limit may not be evaluated. The cover page, table of contents, and any authorized appendices, as outlined herein (i.e., proposed option to utilize DETER as a secondary testbed, resumes for key personnel, and list of any current or pending awards or proposals with DHS), submitted by the offeror are excluded from the page limitation.

(2) Volume 2: No page limitations.

f. Proprietary Marking. Offerors are expected to appropriately mark each page of the proposal that contains proprietary information.

g. Copies:

(1) For Volume 1, Technical Proposal, the submission shall consist of ONE electronic file in portable document format (PDF), readable by IBM-compatible PCs and must be no larger than 10 MB.

(2) For Volume 2, Cost Proposal, the submission shall consist of one electronic file in portable document format (PDF), readable by IB-compatible PCs and must be no larger than 10 MB.

C. **Proposal Content:**

1. Volume 1, Technical Proposal. Volume 1 of the proposal shall be in the form of a technical volume, not to exceed 40 pages, and a cost proposal overview. Compliance with the order and content of sections listed in Volume I is important to assure thorough and fair evaluation of proposals. The submission of other supporting materials with the proposal is strongly discouraged and, if submitted, will not be reviewed. Nonconforming proposals may be rejected without review. The technical proposal shall cover all elements addressed in the white paper. The technical proposal shall include the following:

a. Cover Page. Title the cover page "Volume 1 - Technical Proposal" and also ensure the following information is included:

(1) BAA number, i.e., "BAA 11-02";
(2) Title of proposal;
(3) Name of offeror's organization and offeror's administrative and technical points of contact, including name, address, telephone and facsimile numbers, and email addresses. If multiple organizations are participating, identify the above information for each organization;
(4) Identify whether the offeror (and each organization participating) is a US or foreign owned entity;
(5) Identity of prime offeror and complete list of subcontractors, if applicable;
(6) Type classifications as described in paragraph III.C. above (Type I, Type II, or Type III) that aligns with the proposed technology (should mirror white paper submission and what is identified on the cover page of the cost proposal);
(7) Duration of effort. Separately identify the basic effort and any options. Ensure the total duration does not exceed the timeframe identified in paragraph III.C. for the Type classification assigned to the proposed technology;
(8) In accordance with FAR 4.1201, prospective offerors for contracts and for OTAs involving prototypes (Section 845), shall state the certifications in the Online Representations and Certifications Application (ORCA) at http://orca.bpn.gov have been completed and shall provide the Certification Validity period; and
(9) The signature and title of an authorized representative of the entity submitting the proposal. If multiple organizations are participating, one signature from the principal/leading organization is acceptable.

b. Table of Contents.

c. Official Transmittal Letter. Provide an official transmittal letter with authorizing official signature. For the electronic submission, the letter can be scanned into the electronic proposal. The letter of transmittal shall include, at a minimum, the following:

(1) Whether the proposal has been submitted to a Government agency other than DHS and, if so, shall specify which agency and the date it was submitted.

(2) The preferred vehicle type for DHS S&T to consider for award. For a list of possible vehicles to be awarded as a result of BAA 11-02, refer to paragraph VII.C.1 above.

(3) The required disclosure regarding organizational conflict of interest identified in paragraph XIV.F. below.

(4) A statement that the offeror's proposal is available for award 12 months from the closing date for receipt of proposals.

d. Quad Chart. A quad chart shall be included and shall be in the format identified in paragraph VIII.B.8. above. This chart should be similar to that provided with the white paper; however, minor changes are allowed.

e. Executive Summary. Provide a one-page synopsis of the entire proposal, including a listing of total anticipated costs. This page should include the proposal title and offeror name, along with a description of the scientific, technical, engineering, and management approach being proposed to address the goals of the TTA. It also should describe how the approach is unique, and provide a brief summary of the technology's anticipated performance relative to the TTA goals. This section shall be separable, i.e., it will begin on a new page and the following section shall begin on a new page.

f. Performance Goals: Describe the overall methodology and how it will meet the goals specified in the TTA.

g. Detailed Technical Approach (no more than 15 pages): Describe the proposed design and technical issues. Identify the critical technical issues in the design and concept.

h. Statement of Work (SOW), Schedule, and Milestones: Provide an integrated display for the proposed research, showing each task with major milestones. Include a section clearly marked as the SOW you propose to undertake. It is anticipated that the proposed SOW will be incorporated as an attachment to the resultant award instrument. To this end, proposals must include a severable SOW (i.e., it will begin on a new page and the following section shall begin on a new page) without any proprietary restrictions, which can be removed from the proposal and attached to the contract or agreement award. Task identified herein must correlate to the tasks identified in the cost proposal submission.

i. Testing and Evaluation.

(1) As stated in paragraph IV above, performers in the DHS S&T CSD technical program will be required to test and evaluate their technologies with respect to system performance goals. Accordingly, offerors should consider the specific test and evaluation requirements of the proposed technical solutions. Identify in the proposal the primary test environment to be used to conduct testing and evaluation. If the primary test environment proposed is other than DETER, show clearly how the proposed test environment will better serve the CSD program with respect to system performance goals. Not using the DETER testbed facility will not negatively affect a proposal.

(2) When proposing to use DETER as a secondary testbed as outlined in paragraph IV.E. above, submit as a separate appendix to the technical proposal, a description, in as much detail as possible, of the test and evaluation requirements, plans for facility usage, such as expected hypotheses, testing parameters, and experiment types. The appendix must outline all the elements of testing to occur using DETER (including the additional time needed to perform this testing.

j. Deliverables:

(1) Provide a detailed list and description of all deliverables proposed under this effort, including data, software, and reports consistent with the objectives of the work; along with suggested due dates (calendar days after the effective date of award). The detailed list of deliverables shall include the required deliverables identified in paragraph XIV.H. below.

(2) It is anticipated that the proposed detailed list and description of all deliverables will be incorporated as an attachment to the resultant award instrument. To this end, proposals must include a severable detailed list and description of all deliverables (i.e., it will begin on a new page and the following section shall begin on a new page) without any proprietary restrictions, which can be removed from the proposal and attached to the contract or agreement award.

k. Management Plan: Provide a brief summary of the management plan, including an explicit description of what role each participant or team member will play in the project, and each participant's or team member's past experience in technical areas related to this proposal.

l. Commercialization Plan: Offerors must also include a description in the proposal of their plan for commercializing the technology, or other plans for getting the technology into established transition paths. Technology transition plans that include commercial partnerships are preferred, but transition into the open source community is also acceptable. This request does not entail providing a full business plan, nor does it imply that DHS views commercialization activities as in the scope of this solicitation. The

intent is for offerors to provide evidence that, as part of the technical plan development, consideration has been given to the ultimate commercialization of the outputs of DHS-funded programs. Such considerations would include expected user base, how the technology will be used, and how it will transition in to broad use. Of key importance are the identification of technology diffusion paths that are appropriate for the type and maturity of the technology involved, and any additional factors that might increase the likelihood of it being commercialized. Proposals will be evaluated with other proposals that are submitted to the same TTA (#1 through #14), and have the same Type (I-III) classification.

m. Facilities: List the location(s) where the work will be performed, and the facilities to be used. Describe any specialized or unique facilities which directly affect the effort.

n. Government-Furnished Resources: Provide a brief summary of required information and data which must be provided by the Government to support the proposed work, if any.

o. Cost Summary: For each year of effort, provide the following:

Direct Labor (prime only) – total man-hours
Direct Labor (prime only) – total costs
Direct Material/Equipment Costs (prime only)
Total Travel Costs (prime only)
Total Other Direct Costs (prime only)
Subcontractor (if applicable) – total man-hours (if applicable)
Subcontractor (if applicable) – total of all costs (i.e., one total amount that includes direct labor, material/equipment, travel, other direct costs, indirect costs, fees/profit, etc)
Total Indirect Costs (prime only)
Total Overhead Costs (prime only)
Total G&A (if applicable) (prime only)
Fees or Profit (if applicable) (prime only)
Grand total of all above costs

p. Resumes for Key Personnel: As an appendix, provide resumes and curriculum vitae (CVs) for each of the key personnel proposed. A minimum of two key personnel must be identified.

q. Other DHS Support: As an appendix, provide a list of any current or pending awards or proposals with DHS that pertain to this work, submitted either as a prime contractor, subcontractor/consultant, or teaming partner.

r. Assertion of Data Rights: This section shall be severable, i.e., it will begin on a new page and the following section shall begin on a new page. It is anticipated that the proposed Assertion of Data Rights will be incorporated as an attachment to the resultant

award instrument. To this end, proposals must include a severable Assertion of Data Rights (i.e., it will begin on a new page and the following section shall begin on a new page) without any proprietary restrictions, which can be removed from the proposal and attached to the contract or agreement award.

(1) Provide a summary of any assertions to any technical data or computer software that will be developed or delivered under any resultant award. This includes any assertions to pre-existing results, prototypes, or systems supporting and/or necessary for the use of the research, results, and/or prototype. Any rights asserted in other parts of the proposal that would impact the rights in this section must be cross-referenced. If less than unlimited rights in any Data delivered under the resultant award are asserted, the offeror must explain how these rights in the Data will affect its ability to deliver research data, subsystems and toolkits for integration as set forth below. Additionally, offerors must explain how the program goals are achievable in light of these proprietary and/or restrictive limitations. If there are no claims of proprietary rights in pre-existing data, this section shall consist of a statement to that effect.

(2) Proposals submitted in response to this solicitation shall identify all technical data or computer software that the Offeror asserts will be furnished to the Government with restrictions on access, use, modification, reproduction, release, performance, display, or disclosure. Offeror's pre-award identification shall be submitted as an attachment to its offer and shall contain the following information:

(a) Statement of Assertion. Include the following statement: "The Offeror asserts for itself, or the persons identified below, that the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose only the following technical data or computer software should be restricted:"

(b) Identification of the technical data or computer software to be furnished with restrictions. For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process as specifically as possible (e.g., by referencing specific sections of the proposal or specific technology or components). For computer software or computer software documentation, identify the software or documentation by specific name or module or item number.

(c) Detailed description of the asserted restrictions. For each of the technical data or computer software identified above in paragraph (2), identify the following information:

(i) Asserted rights. Identify the asserted rights for the technical data or computer software.

(ii) Copies of negotiated, commercial, and other non-standard licenses. Offeror shall attach to its offer for each listed item copies of all proposed negotiated license(s), Offeror's standard commercial license(s), and any other asserted restrictions

other than government purpose rights; limited rights; restricted rights; rights under prior government contracts, including SBIR data rights for which the protection period has not expired; or government's minimum rights.

(iii) Specific basis for assertion. Identify the specific basis for the assertion. For example:

- Development at private expense, either exclusively or partially. For technical data, development refers to development of the item, component, or process to which the data pertains. For computer software, development refers to the development of the software. Indicate whether development was accomplished exclusively or partially at private expense.

- Rights under a prior government contract, including SBIR data rights for which the protection period has not expired.

- Standard commercial license customarily provided to the public.

- Negotiated license rights.

(iv) Entity asserting restrictions. Identify the corporation, partnership, individual, or other person, as appropriate, asserting the restrictions.

(3) Previously delivered technical data or computer software. The Offeror shall identify the technical data or computer software that are identical or substantially similar to technical data or computer software that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or subcontract. The Offeror need not identify commercial technical data or computer software delivered subject to a standard commercial license.

(4) Estimated Cost of Development. The estimated cost of development for that technical data or computer software to be delivered with less than Unlimited Rights.

(5) Supplemental information. When requested by the Contracting Officer, the offeror shall provide sufficient information to enable the Contracting Officer to evaluate the offeror's assertions. Sufficient information should include, but is not limited to, the following:

(a) The contract number under which the data or software were produced;

(b) The contract number under which, and the name and address of the organization to whom, the data or software were most recently delivered or will be delivered; and

(c) Identification of the expiration date for any limitations on the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose the data or software, when applicable.

(6) Ineligibility for award. An Offeror's failure to submit or complete the identifications and assertions required above with its offer may render the offer ineligible for award.

2. Volume 2, Cost Proposal. Pursuant to FAR 15.403, certified cost and pricing data will be required prior to contract award. The Cost Proposal shall consist of the following:

a. Cover Page. The use of the SF 1411 is optional. The words "Cost Proposal" should appear on the cover page in addition to the following information:

(1) BAA number, i.e., "BAA 11-02";
(2) Title of proposal;
(3) Name of offeror's organization and offeror's administrative and technical points of contact, including name, address, telephone and facsimile numbers, and email addresses;
(4) Identify whether offeror is US or foreign owned entity;
(5) Identity of prime offeror and complete list of subcontractors, if applicable;
(6) Type classifications as described in paragraph III.C. above (Type I, Type II, or Type III) that aligns with the proposed technology (should mirror white paper submission and what is identified on the cover page of the cost proposal);
(7) Duration of effort. Separately identify the basic effort and any options. Ensure the total duration does not exceed the timeframe identified in paragraph III.C. for the Type classification assigned to the proposed technology.
(8) In accordance with FAR 4.1201, prospective offerors for contracts and for OTAs involving prototypes (Section 845), shall state the certifications in the Online Representations and Certifications Application (ORCA) at http://orca.bpn.gov have been completed and shall provide the Certification Validity period; and
(9) The signature and title of an authorized representative of the entity submitting the proposal.

b. Provide a cost breakdown by task/sub-task using the same tasks identified in the Statement of Work. This part should be consistent with your proposed SOW. Activities such as demonstrations required to reduce the various technical risks should be identified in the SOW and reflected in this part as well.

(1) For each task/sub-task identified, provide a detailed breakdown of costs by fiscal year. The cost breakdown should include, at a minimum, the cost categories identified below.
(a) Direct Labor. Individual labor category or person, with associated labor hours and ***unburdened*** direct labor rates.

(b) Indirect Costs. Fringe Benefits, Overhead, General & Administrative (Expenses), Cost of Money, etc. (***Must show base amount and rate for each element.***)

(c) Travel. Number of trips, destinations, durations, etc. Ensure submission include the anticipated travel identified in paragraph XIV.G.3. below.

(d) Materials. Total direct material that will be acquired and/or consumed during the period of performance should be specifically itemized with costs or estimated costs. Where possible, indicate purchasing method, (e.g., competition, engineering estimate, market survey, etc.). Limit this information to only major items of material (>$25,000) and how the estimated expense was derived. Include major facility requirements such as test ranges or live fire demonstrations. These requirements may address specific facilities, but should also provide details of facility capability requirements and estimates of total facility occupancy and test time. At its discretion, DHS S&T may choose to make bulk purchases of facility time in one or more major test facilities and apportion that test time to program participants.

(e) Other Directs Costs. Any direct costs not included elsewhere, particularly any proposed items of equipment or facilities. List the item, the estimated cost, and basis for the estimate. Equipment and facilities generally must be furnished by the contractor/recipient. Justifications must be provided when Government funding for such items is sought.

(f) Fee/Profit including fee percentage.

(2) Subcontracts. Include subcontractor cost in the detailed breakdown identified in paragraph IX.C.2.b.1. above. Costs should be clearly marked as "prime" or "subcontractor" costs. If the subcontractor costs cannot be included with the above detailed cost breakdown, then the prime contractor must stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor's costs are provided separately in a sealed envelope. The separate subcontractor cost proposal must be as detailed as the offerors's cost proposal and must be submitted with the offeror's proposal.

(3) For proposed technology that is classified as Type I, include the cost for the option to conduct technology demonstrations in an operational environment effort separately from the remainder of the effort. The cost breakdown for this effort shall be provided as detailed as the cost breakdown identified in paragraph IX.C.2.b.1 above.

(4) Offers who elect to include an option for the Government to award DETER as a secondary testbed as outlined in paragraph IV.E. above shall include these costs as an appendix to the cost proposal. The cost breakdown shall be as detailed as the cost breakdown identified in paragraph IX.C.2.b.1 above.

(5) Consultant. Provide consultant agreement or other document which verifies the proposed loaded daily/hourly rate.

D. **Proposal Submissions:**

1. Proposals will not be accepted from any offerors other than those invited to submit proposals. Proposal submissions will not be accepted if the organization has not registered by the due date outlined in paragraph II.E. above.

2. The due date for the submission of proposals is no later than 4:30 P.M. (Local Eastern Time) on **May 26, 2011**. Proposals **WILL NOT BE ACCEPTED** after the established due date.

3. Procedures for submitting a proposal are as follows:

a. After logon to https://baa2.st.dhs.gov, find previous white paper submission in the proposal activity worksheet.

b. Click on the "Create Full Proposal" link within the white paper record, enter a proposal title and add the proposal to the activity worksheet.

c. From the proposal activity worksheet, fill out the requisite fields, upload the proposal files, and then submit. Offerors submitting a proposal will receive confirmation of the submission via e-mail. For additional information download the training guide that can be obtained from the upper left hand corner of the FAQs tab on the logon site.

d. An offeror's proposal submission may be revised until the proposal submission deadline outlined in paragraph II.E. above.

4. No classified proposals (or portions of proposals) will be accepted.

5. In teaming situations, the lead/prime organization must remain the same as what was submitted on the white paper. Any proposal submitted by any organization that was not the lead organization for the white paper submission will not be considered.

6. Proposal submissions will be protected from unauthorized disclosure in accordance with FAR 15.207, applicable law, and DHS regulations.

X. EVALUATION OF WHITE PAPERS AND PROPOSALS.

A. Evaluation Criteria. The evaluation of white papers and proposals will be accomplished through a Peer or Scientific review panel using the following criteria, which are listed in descending order of relative importance.

1. Criterion I. Sound technical and managerial approach to the proposed work, including a demonstrated understanding of the critical technology or engineering challenges required for achieving the goals of the TTA.

2. Criterion II. Potential of the technology/solution for meeting the TTA goals provided in BAA 11-02 resulting in the best ideas and concepts.

3. Criterion III. Qualitative assessment of the commercialization experience and strategy to determine the likelihood that the offeror will be able to deploy a technology and/or solution(s) that can be transitioned effectively to the user community either through commercialization of the technology or through other means.

4. Criterion IV. Capability to perform proposed work and history of performance of the Team in developing related technologies.

5. Criterion V. Each offeror's cost/price proposal will be evaluated for reasonableness and completeness of the proposed contract cost.

B. Evaluation Panel.

1. All properly submitted white papers and proposals that conform to the BAA requirements will be evaluated by a peer or scientific review panel comprised of government technical experts drawn from staff within DHS S&T and other Federal agencies. All government personnel are bound by public law to protect proprietary information.

2. The Government may use selected support contractor personnel to provide administrative assistance to federal employees regarding all aspects of any actions ensuing from this announcement, including supporting federal employees involved in the evaluation of white papers and subsequent proposals. However federal employees will be responsible for actual reviews and evaluations. These support contractors will be bound by appropriate non-disclosure agreements to protect proprietary and source-selection information and are not be permitted to release any source-selection information to third parties, including others in their organization. By submission of a White Paper and/or subsequent Proposal, offerors are hereby consenting access to financial, confidential, proprietary, and/or trade secret markings in the White Paper and/or subsequent Proposal to support contractor personnel.

XI. BASIS OF WHITE PAPER AND PROPOSAL SELECTION.

A. The primary basis for selecting white papers for participation in the proposal phase and selecting proposals for award shall be technical, importance to agency programs, and funding availability. Cost reasonableness and completeness will also be considered to the extent appropriate for white paper submissions and proposals.

B. DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to BAA 11-02.

XII. NOTIFICATION TO OFFERORS OF EVALUATION FINDINGS.

1. Once the white paper evaluation process is complete:

a. Offerors will be notified via e-mail, or in writing, whether the white paper submission is deemed as being "of particular value" to DHS S&T.

b. Offerors who are not invited to submit proposals may request feedback regarding the evaluation findings of submitted white papers. A written request to the Contracting Officer must be received within 3 calendar days of notification of non-selection.

c. For those offerors whose white papers are deemed as being "of particular value" to DHS S&T, the notification will provide an invitation to submit proposals. Only offerors whose white papers are deemed as being "of particular value" to DHS S&T will be invited to submit proposals. ***PROPOSALS WILL NOT BE ACCEPTED FROM ANY OFFERORS OTHER THAN THOSE INVITED TO SUBMIT PROPOSALS***.

2. Once the proposal evaluation process is complete, offerors will be notified via e-mail, or in writing, of selection or non-selection for an award. Offerors not selected for an award may request feedback regarding the evaluation findings of submitted proposals. A written request to the Contracting Officer must be received within 3 calendar days of notification of non-selection.

XIII. APPLICABLE SOLICITATION PROVISIONS AND CONTRACT CLAUSES

In addition to providing the provisions applicable to BAA 11-02, Appendix B identifies the contract clauses that will be pursuant to any resultant award from BAA 11-02. However, the clauses in addition to those included in Appendix B may be applicable and added at the time any resultant award is executed, excluding grants and OTAs.

XIV. OTHER TERMS & CONDITIONS

A. **NAICS.** The North American Industry Classification System (NAICS) code for this announcement is 541712, with a small business size standard of 500 employees.

B. **Central Contractor Registry (CCR).** Successful offerors not already registered in the CCR will be required to register in the CCR prior to award of any grant, contract, cooperative agreement, or, if authorized by law at time of award, OTA. Information regarding CCR registration is available at http://www.ccr.gov/.

C. **Certifications.** As required by paragraph IX.C.1.a.(7), prospective offerors for contracts and, if authorized by law, for OTAs involving prototypes (Section 845), shall complete the Online Representations and Certifications Application (ORCA) at http://orca.bpn.gov and reflect this completion it the proposal submission. Successful offerors will be provided additional information with regards to certification for grants and cooperative agreements proposals.

D. **Subcontracting Plans.** Successful contractor proposals that exceed $650,000, submitted by all but small business concerns, will be required to submit a Small Business Subcontracting Plan in accordance with FAR 52.219-9, prior to award.

E. **Information for White Paper and Proposal Respondents.**

1. BAA 11-02 is for planning purposes only. It will not be construed as an obligation on the part of the Government to acquire any products or services.

2. No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of submission of responses to BAA 11-02 and the Government's use of such information. Respondents to BAA 11-02 may be requested to provide additional information based on their submittals. Unnecessarily elaborate responses containing extensive marketing materials are not desired.

3. Technical and cost proposals, or any other material, submitted in response to BAA 11-02 will not be returned. However, depending on the markings on the proposal, DHS S&T will adhere to FAR policy on handling source selection information and proprietary proposals. It is the policy of DHS S&T to treat all proposals as sensitive competitive information, and to disclose their contents only for the purpose of evaluation.

F. **Organizational Conflict of Interest.**

1. Offerors who have existing or pending contract(s) to provide scientific, engineering, technical and/or administrative support directly to DHS S&T may be considered to have actual or potential conflict of interest, resulting in the one or more offerors with the potential to attain an unfair competitive advantage.

2. If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the Offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the Offeror and include the appropriate provisions to mitigate or avoid such conflict in the contract awarded. After discussion with the Offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the Offeror may be found ineligible for award.

3. Disclosure. Each offeror will be required to represent, as part of its proposal and to the best of its knowledge that: (1) It is not aware of any facts which create any actual or

potential organizational conflicts of interest relating to the award of this contract; or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph D. of this provision.

4. Mitigation/Waiver. If an Offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the offeror shall submit a mitigation plan to the Contracting Officer for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan.

5. Other Relevant Information. In addition to the mitigation plan, the Contracting Officer may require further relevant information from the Offeror. The Contracting Officer will use all information submitted by the Offeror, and any other relevant information known to DHS, to determine whether an award to the Offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

6. Corporation Change. The successful Offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

7. Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

G. **Required Deliverables Applicable to Any Award Resulting From BAA 11-02.** The following *minimum* deliverables will be required in all awards resulting from BAA 11-02:

1. Monthly Program Report. A brief narrative report (not more than two pages) will be electronically submitted to the Program Manager within one week after the last day of each month throughout the performance period of the contract. The monthly report will describe:

a. The previous calendar month's activity;
b. The technical progress achieved against goals;
c. The difficulties encountered;
d. Recovery plans (if needed);
e. Explicit plans for the next calendar month; and,
f. Financial expenditures (including expenditures during the past calendar month period plus cumulative expenditures, and projected expenditures for the coming calendar month).

2. Final Technical Report.

a. For a final report, the contractor shall provide a technical report of work performed during the period of performance, delivered no later than the last day of the

period of performance. The final report shall be a cumulative, stand-alone document that describes the work of the entire test and evaluation period leading up to it.

b. It shall detail how the design prototype was refined or otherwise prepared for the test and evaluation program and, if applicable, why such refinements or preparations were undertaken. It must include any technical data gathered, such as measurements taken, models developed, simulation results, and formulations developed.

c. The final report shall include a summary of all performance goals versus performance achieved during the program, either measured or otherwise substantiated. The final report shall discuss all variances from the performance goals versus performance achieved, including reasons or theories for variances.

d. If applicable, it will provide a discussion of how the offeror might meet any unmet performance goals under a future effort.

e. The final report is required to include "lessons learned" from the effort, and recommendations for future research, development, or testing that would lead to success in meeting the performance goals.

f. The final report shall provide a comprehensive and detailed account of all funds expended.

3. Project Conferences, Meetings, and Reviews. A maximum of three program status reviews will be held annually to provide a forum for reviews of the latest results from experiments and any other incremental progress towards the major demonstrations. These meetings will be held at various sites throughout the country. For costing purposes, offerors should assume that one meeting will be held in Washington, D.C., and one meeting will be held at the awardee's facility. Interim meetings are likely, but these will be accomplished via video telephone conferences, telephone conferences, or Web-based collaboration tools.

H. **Government Property, Government Furnished Equipment (GFE), and Facilities.**

1. The Government may provide government-furnished equipment (GFE), resources (GFR), information (GFI), or services (GFS) under the terms of each negotiated contract or agreement. GFE, GFR, GFI, or GFS requested by an offeror must be factored into the offeror's project cost. Each offeror must provide a very specific description of any equipment or hardware it needs to acquire to perform the work. This description should indicate whether or not each particular piece of equipment or hardware will be included as part of a deliverable item under the resulting award.

2. In addition, this description should identify the component, nomenclature, and configuration of the equipment or hardware that it is proposed to purchase for this effort. The Government wants to have the contractor purchase the equipment or hardware for deliverable items under its contract. It will evaluate case-by-case the purchase, on a direct

reimbursement basis, of special test equipment or other equipment, not included in a deliverable item will be evaluated for allowability on a case-by-case basis. Maximum use of Government integration, test, and experiment facilities is encouraged in each of the offeror's proposals.

3. Government research facilities may be available, and should be considered as potential GFE. These facilities and resources are of high value, and some are in constant demand by multiple programs. The use of these facilities and resources will be negotiated as the program unfolds. Offerors should explain which of these facilities they recommend and why.

I. **Security Classification.** No Classified White Papers or Proposals (or portions of proposals) will be accepted.

J. **SAFETY Act.** As part of the Homeland Security Act of 2002, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY" Act). The SAFETY Act puts limitations on the potential liability of firms that develop and provide qualified anti-terrorism technologies. DHS S&T, acting through its Office of SAFETY Act Implementation (OSAI), encourages the development and system prototype development in an operational environment of anti-terrorism technologies by making available the SAFETY Act's system of "risk management" and "liability management." Offerors submitting proposals in response to BAA 11-02 are encouraged to consider submitting SAFETY Act applications for their existing technologies. Offerors are invited to contact OSAI for more information, at 1-866-788-9318 or helpdesk@safetyact.gov. Offerors also can visit OSAI's Web site at www.safetyact.gov.

XV. LIST OF APPENDICES

Appendix A - Technical Topic Areas #1 through #14
Appendix B - Applicable Provisions and Clauses
Appendix C - Acronyms

APPENDIX A – TECHNICAL TOPIC AREAS (TTAs)

TTA #1: Software Assurance

a. The nation's critical infrastructure (energy, transportation, telecommunications, banking and finance, and others), businesses, and services are extensively and increasingly controlled and enabled by software. Vulnerabilities in that software put those resources at risk. The risk is compounded by software size and complexity, the ways in which software is developed and maintained, the use of software produced by unvetted suppliers, and the interdependence of software systems. Software quality addresses the presence of internal flaws and vulnerabilities in software threatening its correct or predictable operation and use. Software assurance deals with the root of the problem by improving software security.

b. The cost of software program failures is staggering. In 2002, COMPUTERWORLD reported that *"Software bugs are costing the U.S. economy an estimated $59.5 billion each year, with more than half of the cost borne by end users and the remainder by developers and vendors, according to a new federal study. Improvements in testing could reduce this cost by about a third, or $22.5 billion, but it won't eliminate all software errors, the study said. Of the total $59.5 billion cost, users incurred 64% of the cost and developers 36%."* [1]

c. Threats must be addressed throughout the software development process, with an emphasis on the entire software engineering lifecycle -- including requirements, design, specification, implementation, test/evaluation, system prototype demonstration, operation, maintenance, and ultimate decommissioning. Threats to a system in operation include everything that can prevent critical applications from satisfying their intended requirements, including insider and outsider misuse, malware and other system subversions, software flaws, hardware malfunctions, human failures, and environmental disruptions. Indeed, systems sometimes fail without any external provocation, as a result of design flaws, implementation bugs, or misconfiguration.

d. The overall stability, reliability and resilience of software have not kept pace in these increasingly demanding environments. New vulnerabilities in fielded software are found daily, many of which are not known or reported to the vendor. New and innovative methods, services, and capabilities in the build, test, and analysis phases are needed to improve the quality and reliability of software used in the nation's critical infrastructures.

e. This TTA has two parts: (1) research and development of new tools and techniques for software analysis; and (2) applying new and existing capabilities in test and evaluation activities.

(1) New tools. Techniques that require access to source code, as well as binary-only techniques, are in scope for this program. Recent work in software model-checking shows promising results in discovering vulnerabilities, defects, and other types of weaknesses in software. New forms of static analysis are within scope, as well as new runtime monitoring techniques. Innovative combinations of these techniques are strongly encouraged to synergize the benefits of each while minimizing the difficulties.

(2) Application of new and existing capabilities in test and evaluation activities - These activities may take one of several forms:

1http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,72245,00.html

(a) Analyzing large code bases, including operating systems, development and execution environments, distributed computing software, and middleware systems.

(b) Benchmarking new tools against analysis results previously documented and recorded for common programs and applications and for which a database of vulnerabilities is established. Examples of targeted applications include, but are not limited to, email programs, web servers, web browsers, and file transfer applications.

(c) Providing a comprehensive test and evaluation service that applies a broad array of new and existing analysis tools in combination to test and evaluate software across relevant platforms and environments.

f. The program seeks to couple activities funded in this TTA with a new effort called "Homeland Open Security Technology (HOST)", whose goal is to facilitate Government-wide secure information technology (IT) solutions based on open source technologies. HOST will enable more effective access to vetted open source and related technologies used within the Government. One goal in this initiative is to include a process of rigorous test and evaluation of software in source and binary form relying heavily on automated processes. More information on HOST can be found at http://www.cyber.st.dhs.gov. Also, proposals addressing part (2) of this TTA are encouraged to consider how their activities can tie-in to TTA 14 addressed later in this solicitation.

References for TTA #1:

- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #1, p. 6, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 1, p. 83, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." Secure Software Engineering, p. 81, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- INFOSEC Research Council. "Hard Problems List." Problem #4 – Building Scalable Secure Systems, p. 19, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- President's Information Technology Advisory Committee (PITAC). "Cyber Security: A Crisis of Prioritization." Research Priority #3, p. 39, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- Computing Research Association. "Four Grand Challenges in Trustworthy Computing." Challenge #2, p. 17, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- White House. "The National Strategy to Secure Cyberspace." Priority II, Area B, Topic #2, p. 32, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- Information Institute for Infrastructure Protection (I3P). "Cyber Security Research and Development Agenda." Research Area #3, p. 18, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Trust in Cyberspace." Recommendation #2, p. 244, 1999. <http://www.cyber.st.dhs.gov/documents.html>

TTA #2: Enterprise-Level Security Metrics

a. Defining effective information security metrics has proven difficult, even though there is general agreement that such metrics could allow measurement of progress in security measures and, at a minimum, rough comparisons of security between systems. Metrics underlie and quantify progress in many other system security areas. "You cannot manage what you cannot measure," as the saying goes; the lack of sound and practical security metrics is severely hampering progress both in research and engineering of secure systems. However, general community agreement on meaningful metrics has been hard to achieve. This is due in part to the rapid evolution of IT, as well as the shifting locus of adversarial action.

b. Security itself is difficult to define. One view is to define it as the probability that a system under attack will meet its specified objectives for a specified period of time in a specified environment. Note that this definition incorporates specifications of both the system objectives and the system environment, which would include some notion of a threat model. Though this type of probability metric has been computed for system reliability and computed for systems as risk assessments, the accuracy of such assessments is questionable.

c. Security metrics are difficult to develop because they typically try to measure the absence of something negative, e.g., lack of any unknown vulnerabilities in systems and lack of adversary capabilities to exploit both known and unknown vulnerabilities. This is difficult since there are always unknowns in the system and the landscape is dynamic and adversarial. The community needs better definitions of the environment and attacker models to guide risk-based determination. These are difficult areas, but progress is achievable.

The following definition from the National Institute of Standards and Technology (NIST) may provide useful insights:

"IT security metrics provide a practical approach to measuring information security. Evaluating security at the system level, IT security metrics are tools that facilitate decision making and accountability through collection, analysis, and reporting of relevant performance data. Based on IT security performance goals and objectives, IT security metrics are quantifiable, feasible to measure, and repeatable. IT security metrics provide relevant trends over time and are useful in tracking performance and directing resources to initiate performance improvement actions."

d. Along with the systems, component-level metrics and the technology-specific metrics that are continuing to emerge with new technologies year after year, it is essential to have a macro-level view of security within an organization. A successful research program in metrics should define a security-relevant science of measurement. The goals should be to develop metrics to allow decision-makers to answer the following questions.

(1) How secure is my organization?
(2) Has our security posture improved over the last year?
(3) To what degree has security improved in response to changing threats and technology?
(4) How do we compare with our peers?
(5) How secure is this product or software that we are purchasing or deploying?
(6) How does that product or software fit into the existing systems and networks?
(7) What is the marginal change in our security, given the use of a new tool or practice?

(8) How much security is enough given the current/project threats?
(9) What is the cost of not implementing security improvements?
(10) How robust is my system against cyber threats, misconfiguration, and environmental effects? (Note: This is especially important for critical infrastructures.)

e. Enterprise-level security metrics (ELMs) address the security posture of an organization. The enterprise is not the Internet as a whole, but can scale in size from a large corporation (or department of the Federal government) down to the Small Office/Home Office (SOHO). For our purposes, an enterprise has a single point of decision authorized to use ELMs to rationally select among alternatives to improve the security posture of their enterprise. ELMs support decisions such as whether adoption of one technology or another improves enterprise security. ELMs also provide the basis for accurate situational awareness of the enterprise's security posture.

f. In this discussion, DHS S&T is restricting the scope to enterprise level in order to define metrics relevant to hosts within an enterprise, and roll up host level measurements to an enterprise level. In other words, the goals of ELM are to understand security of an end system and roll this up to understand enterprise security as a whole with a goal of using these measurements to guide rational investment in security. If these ELM goals are met, then extensions to other related cases, such as Internet Service Providers (ISP) and their customers, should be feasible.

g. Good security metrics are required to make good decisions about how to design security countermeasures, to choose between alternative security architectures, and to improve security during design and operations. So, in essence, measurement can be viewed as a decision aid. The lack of sound and practical security metrics is severely hampering progress in both the research and engineering of secure systems.

h. Some qualities of a good metric include:

(1) Ability to measure the right thing (such as supporting the decisions that need to be made).
(2) Quantitatively measurable, i.e., damages in dollars of profit loss.
(3) Capability to be measured accurately.
(4) Ability to be validated against ground truth.
(5) Confidence level one has in the assertions made within the framework of the metric.

i. To these above qualities, one could also add the following desirable properties:

(1) Inexpensive both in time and cost to execute.
(2) Able to be refereed independently.
(3) Repeatable so that the results are independent of the analyst performing the measurement.
(4) Scalable from small, single computer systems to large, nation-scale enterprise networks.

j. The goal of this TTA is to develop security metrics and the supporting tools and techniques to make them practical and useful as decision aids. Assessing these systems is a costly and labor-intensive exercise which is largely *ad hoc* today (with the exception of a few highly trusted systems). The end result of this lack of system assessment capability is that systems are routinely deployed without a coherent understanding of their cyber security characteristics or a set of management guidelines for maintaining an adequate security posture. This program seeks research ideas that can remedy this situation. Following the NIST definition, proposed approaches will be evaluated to the degree to which

they can address the questions and criteria above and address the research agendas included in the References below.

k. Proposals in this TTA are encouraged to look for opportunities in applying new metrics to existing security processes and operational environments. Studying the impact of new metrics for effectiveness of security controls, assessing risk, estimating cost, and regulatory compliance, are among the many drivers for experimental integration and system prototype demonstration in an operational environment.

References for TTA #2:

- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 2, p. 13, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #6, p. 19, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 3, p. 133, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." Metrics, p. 63, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- INFOSEC Research Council. "Hard Problems List." Problem #8 – Enterprise-Level Security Metrics, p. 31, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- President's Information Technology Advisory Committee (PITAC). "Cyber Security: A Crisis of Prioritization." Research Priority #9, p. 45, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- Computing Research Association. "Four Grand Challenges in Trustworthy Computing." Challenge #3, p. 20, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- Information Institute for Infrastructure Protection (I3P). "Cyber Security Research and Development Agenda." Research Area #7, p. 33, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Trust in Cyberspace." Recommendation #2, p. 251, 1999. <http://www.cyber.st.dhs.gov/documents.html>
- National Institute of Standards and Technology. "Information Technology Laboratory Bulletin August 2003." http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm

TTA #3: Usable Security

a. Although the problem of achieving usable security is universal — it affects everyone, and everyone stands to benefit enormously if usability is successfully addressed as a core aspect of security — it affects different users in different ways, depending on applications, settings, policies, and user roles. The guiding principles may indeed be universal, but there is certainly no general one-size-fits-all solution.

b. While the importance of security technology is widely recognized, it is often viewed merely as a hindrance to productivity; security is poorly understood by non-experts, and the consequences of disabled or weakened security controls are often indirect and not immediately felt. The worst effects may be felt by those not directly involved, e.g., credit-card fraud, leading users to question the value of security technology at all.

c. At the same time, consciousness of security issues is becoming more widespread and technology developers are paying increasing attention to security in their products and systems. However, usability in general appears not to be much better understood than security is by software practitioners. This makes the problem of usable security even more challenging since it combines two problems that are difficult to solve individually.

d. Typically, as the security of systems increases the usability of those systems tends to decrease because security enhancements are commonly introduced in ways that are difficult for users to comprehend and that increase the complexity of users' interactions with systems. Any regular and frequent user of the Internet will readily appreciate the challenge of keeping track of dozens of different passwords for dozens of different sites. Many users also are frustrated by security pop-up dialogs that offer no intuitive explanation of the apparent problem and, moreover, appear completely unable to distinguish between normal legitimate activity, such as reading e-mail from a friend, and from a phishing attempt.

e. A few illustrative examples of usable security from the current state of the practice may help to illuminate challenges in usable security and identify some promising directions from which broader lessons may be drawn:

(1) Passwords. While the security pitfalls of poorly implemented password schemes have been extensively documented over the years, when used wisely passwords are both effective and well understood by users. Tools that help users select good passwords and manage their passwords have enhanced both usability and security.

(2) DomainKeys Identified Mail (DKIM). DKIM is e-mail authentication technology that allows e-mail recipients to verify whether messages that claim to have been sent from a particular domain actually originated there. It operates transparently to end users and makes it easier to detect possible spam and phishing attacks, both of which often rely on domain spoofing.

(3) Security "pop-up" dialogs. No matter how much effort is put into making security controls automated and transparent, there are inevitably situations that require the user to make a security-related decision. Unfortunately today, user involvement appears to be required too often and usually in terms that non-technical users have difficulty understanding, leading to the frustrating effects noted earlier.

(4) CAPTCHA *systems*. A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a challenge-response mechanism intended to ensure that the respondent is a human and not a computer. CAPTCHAs are familiar to most Web users as distorted images of words or other character sequences that must be input correctly to gain access to some service (such as a free e-mail account). To make a CAPTCHA effective for distinguishing humans from computers, solving a CAPTCHA must be difficult for computers, but relatively easy for humans. This balance has proven difficult to achieve, resulting in CAPTCHAs that are either breakable by computers or too difficult for humans.

f. People use systems to perform various tasks toward achieving some goal, and unless the tasks at hand are themselves security related, having to think about security interferes with accomplishing the user's main goal. Security as it is typically practiced in today's systems increases complexity of system use, which often causes confusion and frustration for users. When the relationship between security controls and security risks is not clear, users may simply not understand how best to interact with the system to accomplish their main goals while minimizing risk. Even when there is some appreciation of the risks, frustration can lead users to disregard, evade, and disable security controls, thus negating the potential gains of security enhancements.

g. Security must be usable by non-technical users, experts, and system administrators. Put another way, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security. The need for usable security is increasingly being recognized, as is the fact that usable security is a challenging problem. In attempting to address the challenges of usability and security, several guiding principles may help.

h. The following dimensions are a useful subdivision for formulating responses to this TTA. The major dimensions of this TTA include:

(1) Interface design.
(2) Science of evaluation for usable security.
(3) Tool development.

i. Additional suggestions and recommendations of potential research areas for usable security solutions can also be found in the references below.

References for TTA #3:

- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 11, p. 90, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #3, p. 13, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 3, p. 124, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." Security Across the IT Lifecycle, p. 86, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- President's Information Technology Advisory Committee (PITAC). "Cyber Security: A Crisis of Prioritization." Research Priority #5, p. 41, 2005. <http://www.cyber.st.dhs.gov/documents.html>

TTA #4: Insider Threat

a. Cybersecurity measures are often focused on threats from outside an organization, rather than threats posed by untrustworthy individuals inside an organization. However, insider threats are the source of many losses in many critical infrastructure industries. In addition, well-publicized intelligence community moles such as Aldrich Ames have caused enormous and irreparable harm to national interests. This TTA focuses on insider threats to our cyber systems, and presents a high-impact research program that could aggressively curtail some aspects of this problem. At a high level, opportunities exist to mitigate insider threats through aggressive profiling and monitoring of users of critical systems, "fishbowling" suspects, "chaffing" data and services by users who are not entitled to access, and finally "quarantining" confirmed malevolent actors to contain damage and leaks while collecting actionable counter-intelligence and legally acceptable evidence.

b. An insider threat can be defined as the potential damage to the interests of an organization by a person(s) who is regarded, falsely, as loyally working for or on behalf of the organization, or who inadvertently commits security breaches. Within the IT environment of networks, systems, and information, an organization can have both implicit and explicit security policies. In this environment, an insider threat can be more narrowly defined as the potential violation of system security policy by an authorized user. Although policy violations can be the result of carelessness or accident, the core concern is deliberate and intended actions such as malicious exploitation, theft, or destruction of data, or the compromise of networks, communications, or other IT resources.

c. Detection involves differentiating suspected malicious behavior from normal as well as unusual yet acceptable behavior. Mitigation of the insider threat involves a combination of deterrence, prevention, and detection. Government communities are environments in which access to classified information is available to appropriately cleared members. One of the most harmful and difficult to detect threats to information security is the trusted insider or group of insiders who use privileges in a malicious manner to disrupt operations, corrupt data, exfiltrate sensitive information, or compromise IT systems. Loss of or damage to such operations or information will ultimately compromise the Nation's ability to protect and defend against future attacks, and to safeguard critical infrastructure assets. In fact, some of the most damaging attacks against the government have been launched by trusted insiders. Such attacks will become an increasingly serious threat as increased information sharing results in greater access to, and distribution of, sensitive information. The private sector, where corporations maintain valuable and highly sensitive proprietary information, and where banking institutions manage the flow of and access to electronic funds, share similar concerns over nefarious insider activity. Techniques to mitigate the insider threat typically focus on monitoring systems to identify unauthorized access, establish accountability, filter malicious code, and track data pedigree and integrity. Additionally, there are organizational based mitigation systems which focus upon the culture and climate of the organization which may contribute to movement from thoughts of malicious behavior to actual action. Emotional crises as well as motivational issues could create a personal or group environment where the decision to engage in malicious behavior seems appropriate. While an array of partial measures exists for countering the insider threat, these measures are limited in scope and capabilities.

d. Among the challenges that add to the difficulty of this problem are:

(1) The scale and diversity of the computing infrastructure, in terms of numbers and types of platforms, missions supported, infrastructure architectures and configurations, and worldwide geographic distribution.

(2) The size, variety, and fluidity of the workforce in general and, in the case of government initiatives, the need to interface with partners from industry and other governments, state, local, or foreign.

(3) The variety of highly complex computer security environments that range from unclassified systems to classified networks, and from private-sector systems and networks that support business and electronic commerce to the process control systems of critical infrastructure.

(4) Policy discovery, the process by which the kinds of access permitted to insiders, is difficult to formulate.

(5) Range of behavioral propensities or triggers which lead to malicious action are difficult to understand within the context of insider's knowledge, skills, and experience; environment within which an insider is working; security culture of the organization; and potential recruiting methods of those who would do harm to the organization.

(6) Behaviorally based algorithms combining technical computer-interface actions with personal, human-factors based actions are methodologically challenging.

(7) Human factor issues with regard to dealing with the variety of attacks from outside the organization which are facilitated by insiders are unexplored.

e. The trusted insider operates within this large interconnected world of information systems relatively unchecked and unmonitored, beyond the basic security mechanisms used primarily to detect non-trusted outsiders and prevent them from penetrating and exploiting information assets. Such factors make insider threat a complex problem that is beyond the scope of commercially available tools.

f. The insider threat is today mostly addressed with procedures such as awareness training, background checks, good labor practices, identity management and user authentication, limited audits and network monitoring, two-person controls, application-level profiling and monitoring, and general access controls. However, these procedures are not consistently and stringently applied, because of high cost, low motivation, and limited effectiveness. For example, large-scale identity management can accomplish a degree of non-repudiation and deterrence, but does not actually prevent an insider from abusing granted privileges.

g. The beneficiaries of this research range from the national security bodies operating the most sensitive classified systems to homeland security officials who need to share sensitive-but-unclassified/controlled unclassified information (CUI) information and to healthcare, finance, and many other sectors where sensitive and valuable information is managed. In many systems, such as those operating critical infrastructures, the integrity, availability, and total system survivability are of highest priority and can be compromised by insiders.

h. Beneficiary needs may include: tools and techniques to prevent and detect malicious insider activity throughout the entire system lifecycle; approaches to minimize the negative impact of malicious insider actions; education and training for safe computing technology and human peer detection of insider abuses; and systems that are resilient and can effectively remediate detected insider exploits. Of

particular interest will be the ability to deal with multiple colluding insiders – including detecting potential abuses and responding to them.

i. Approaches for coping with insider misuse can be categorized into six areas:

(1) Collect and Analyze (monitoring).
(2) Detect (provide incentives and data).
(3) Deter (prevention should be an important goal).
(4) Protect (maintain operations and economics).
(5) Predict (anticipate threats and attacks.
(6) React (reduce opportunity, capability, and motivation and morale for the insider).

j. To address the growing concern of insider threats, this TTA seeks more advanced R&D solutions to provide needed capabilities to address these six areas as outlined above and also described in the references below.

References for TTA 4:

- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 4, p. 29, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #4, p. 15, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 5, p. 185, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." Insider Threat Detection and Mitigation, p. 39, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- INFOSEC Research Council. "Hard Problems List." Problem #2 – Insider Threat, p. 13, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- President's Information Technology Advisory Committee (PITAC). "Cyber Security: A Crisis of Prioritization." Research Priority #4, p. 40, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- Computing Research Association. "Four Grand Challenges in Trustworthy Computing." Challenge #2, p. 19, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- White House. "The National Strategy to Secure Cyberspace." Priority III, Area A, Topic b, p. 40, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- Information Institute for Infrastructure Protection (I3P). "Cyber Security Research and Development Agenda." Research Area #3, p. 9-12, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Trust in Cyberspace." p. 112-113, 1999. <http://www.cyber.st.dhs.gov/documents.html>

TTA #5: Secure, Resilient Systems and Networks

a. Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. Part of the survivability attribute of systems and networks includes being secure and resilient to attack. This is meaningful, in practice, only with respect to well-defined mission requirements against which the survivability can be evaluated and measured.

b. Time-critical Systems are systems that require response on non-human timescales to maintain survivability, i.e., continuing to operate under relevant adversities. In these systems, human response is generally infeasible due to a combination of the complexity of the required analysis and the associated time constraints. This program uses the following definition:

"With respect to survivability, a time-critical system is a system for which faster-than-human reaction is required to avoid adverse mission consequences and/or system instability in the presence of attacks, failures, or accidents."

c. Of particular interest here are systems for which impaired survivability would have large-scale consequences, particularly in terms of the number of affected people. Examples of such systems include electric power grids and other critical infrastructure systems, regional transportation systems, large enterprise transaction systems, and major websites. Whereas impaired survivability for some other types of systems may have severe consequences for a small number of users, these "smaller impact systems" are not explicitly included in the scope of this topic. Examples of such systems are medical devices, individual transportation systems, home desktop computers, and isolated embedded systems. Such systems are not always designed for an adequate level of survivability, but it is a less challenging problem to address than for large and distributed systems. However, common-mode failures of large numbers of small systems, e.g. a vulnerability in a common type of medical device, could have large-scale consequences.

d. Security and resilience are central properties to be considered. Security and resilience connect directly to the "in a timely manner" aspect of the above definition of survivability. In some systems, failure to fulfill a mission for even fractions of a second could have severe consequences. In other types of systems, downtime for several minutes could be acceptable. In some other systems, system stability could be threatened if faults are not handled on faster-than human timescales.

e. Today's systems are under constant attack from all directions and the malicious software (malware) being used by adversaries is having an impact on the ability of our systems and networks to maintain secure states and a resilient posture.

f. Approaches to ensure secure and resilient networks in the future require research and development in the area of survivability, and defending against malware. Research and development areas for survivable systems and networks to be explored include:

(1) Protect (protection that does not involve human interaction). Protection topics include:

(a) Understanding how to balance confidentiality and integrity against timely availability.

(b) New communication protocols that are designed for survivability.

(c) Understanding how core functions of the system can be isolated from functions that can be attacked, so that the time critical properties of the core functions are preserved even when the system is attacked.

(d) Exploring how real redundancy can be achieved with assurance to make sure that single points of failure are not present.

(e) Exploring the trade-off in networks between in-band and out-of-band control with respect to survivability, time criticality, and economics.

(f) Exploring containment technology that enables: tolerating malware (for example, safely doing a trusted transaction from a potentially untrusted system); investigating "safe sandbox" techniques for critical transactions; and tolerating a residual level of ongoing compromise within components and subsystems of a larger system. This direction recognizes that malware is part of the environment, and secure operation in the presence of malware is essential.

(2) Detect. Sophisticated and reliable detection methods are required to detect when the survivability of a time-critical system is at risk. This requires run-time methods to detect loss of time-critical system properties such as degradation, and predict potential consequences. The following topics need investigation:

(a) Self-diagnosis (heartbeats, challenge-response, built-in monitoring of critical functions, detection of process anomalies).

(b) Intrinsically auditable systems (systems that are by design instrumented for detection).

(c) Protection of the detection mechanisms, to make sure the mechanism itself cannot be disabled or tricked into reaction.

(3) React and Recover. When survivability is determined to be at risk, reactions should ensure that survivability is preserved. Reactive approaches to be investigated include:

(a) Graceful degradation of service (connection with mission understanding requirements).

(b) System change during operation (to break adversarial planning, to make planned attacks irrelevant).

(c) The coordination of reaction with supporting services.

(d) Bringing undamaged/repaired components back online via autonomous action (no human intervention). This includes reevaluation of component status and communication flows.

g. The absence of meaningful requirements for survivability is a serious gap in practice and is reflected in various gaps in research. For example, the inability to specify requirements in adequate detail and completeness, and the inability to determine whether specifications and systems actually

satisfy those requirements. This TTA is focused to address the critical areas mentioned above, especially as they apply to critical infrastructure. It is expected that research in this TTA will be focused in areas of both basic and applied research.

References for TTA 5:

- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 7, p. 57, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #2, p. 9, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 5, p. 199, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." Fault Tolerant and Resilient Systems, p. 83, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- INFOSEC Research Council. "Hard Problems List." Problem #3 – Availability of Time-Critical Systems, p. 16, and Problem #4 – Building Scalable Secure Systems, p. 19, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- President's Information Technology Advisory Committee (PITAC). "Cyber Security: A Crisis of Prioritization." Research Priority #4, p. 40, and Research Priority #6, p. 42, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- Computing Research Association. "Four Grand Challenges in Trustworthy Computing." Challenge #4, p. 23, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- White House. "The National Strategy to Secure Cyberspace." Priority II, Area C, Topic #1, p. 35, 2003. <http://www.cyber.st.dhs.gov/documents.html>
- Information Institute for Infrastructure Protection (I3P). "Cyber Security Research and Development Agenda." Research Area #4, p. 23, 2003. <http://www.cyber.st.dhs.gov/documents.html>

TTA #6: Modeling of Internet Attacks

a. This TTA researches, develops and applies modeling and analysis capabilities to predict the effects of cyber attacks on Federal Government and other critical infrastructures. Two main areas are identified: malware and botnets; and situational understanding and attack attribution.

b. **Malware and Botnets.**

(1) Malware and botnet activity in recent months and years has intensified across the Internet and other critical infrastructures, with recent events, such as Conficker and Stuxnet, demonstrating the clear and present threat posed that is intelligent, adaptive, and effective at scale over increasingly shorter time periods.

(2) The technical problems are, wherever possible: to avoid allowing malware onto a platform (prevention); to protect systems from infection when malware is in the system's environment (protection); to detect malware that has been installed (detection); analyze malware's infection, propogation, destructive mechanisms, and to monitor and identify its source (analysis); and to remove malware once it has been installed and identify mechanisms to prevent future outbreaks (reaction/remediation).

(3) Among the problems to be addressed in malware and botnets, the following research and development directions are encouraged:

(a) Internet-scale emulation of observable malware, specifically botnets and worms, at Internet scales with goals including helping to identify weaknesses in the malware code and how it spreads or reacts to outside stimuli.

(b) New approaches in malware and botnet detection, identification and visualization, and automated binary analysis.

(c) Malware repository creation and sharing - Collaborative detection may involve privacy-preserving security information sharing across independent domains. This may involve sharing malware samples, metadata of a sample, and/or experiences with appropriate access controls.

(d) Robust security against operating system exploits, such as binary-exploit malware targeting the operating system.

(e) Remediation of systems infected at levels ranging from the user level down to the root level, possibly including built-in diagnostic instrumentation and virtual machine (VM) introspection providing embedded digital forensics.

(4) Technologies developed under this topic must perform their functions within legal and ethical boundaries. It is expected that the resultant tools would be commercialized and made available to critical infrastructure providers in addition to government network operations.

(5) R&D areas for defending against malware to ensure secure and resilient networks include:

(a) Prevent: Prevent the production and propagation of malware.

(b) Protect: Protect systems from infection when malware is in the system's environment.

(c) Detect: Detect malware as it propagates on networks, detect malware infections on specific systems.

(d) Analyze: Analyze malware's infection, propagation, and destructive mechanisms.

(e) React: Remediate a malware infection and identify mechanisms to prevent future outbreaks.

c. **Situational Understanding and Attack Attribution.**

(1) Situational understanding and attack attribution are critical capabilities to attain over the long term in order to effectively deal with Internet attacks.

(2) Situational understanding is information scaled to one's level and areas of interest. It comprehends one's role, environment, the adversary, mission, resource status, what is permissible to view, and which authorities are relevant. The challenge is the path from massive data to information to understanding, allowing for appropriate sharing at each point in the path. Situational understanding includes the state of one's own system from a defensive posture irrespective of whether an attack is taking place. It is critical to understand system performance and behavior during non-attack periods, in that some attack indicators may be observable only as deviations from "normal behavior". Situational understanding also encompasses both the defender and the adversary. The defenders must have adversary models in order to predict adversary courses-of-action based on the current defensive posture.

(3) Attribution is defined as determining the identity or location(s) of an attacker or an attacker's intermediary, or even the instigator of the attack. Attribution includes the identification of intermediaries, though an intermediary may or may not be a willing participant in an attack. Accurate attribution supports improved situational understanding, and is therefore a key element of research in this area. Appropriate attribution may often be possible only incrementally, as situational understanding becomes clearer through interpretation of available information.

(4) Understanding the attack is essential for defense, remediation, attribution to the true adversary or instigator, hardening of systems against similar future attacks, and deterring future attacks. In addition, the more serious attacks now occur at two vastly different time scales. The classic fear is cyber attacks that occur faster than human response times. Those attacks are still of concern. However, another concern is "low and slow" attacks that break the attack sequences into a series of small steps spread over a long time period. Achieving situational awareness for these two ends of the continuum is likely to require very different approaches.

(5) Among the problems to be addressed in this sub-topic area, the following directions are encouraged:

(a) Collect and store relevant data: Understand how to identify, collect and ultimately store data appropriate to the form of situational awareness desired.

(b) Analysis on heterogeneous data sources at large scale, using effective filtering techniques to remove irrelevant data, and supporting a variety of granularities, repeated patterns of interaction over long periods, and unexpected connections between companies and individuals.

(c) Novel approaches to presentation of large scale data, including scalable visualization, visualization with accurate geolocation, and zoomable visualization at varying levels, maintaining the ability to delve into the original data as well as broaden out to a high level people-aware view.

(d) Collaborative collection of non-open data, and the subsequent vetting, archiving, correlation, and generation of useful metadata.

(e) Cross-organizational boundary sharing of situational understanding.

(f) Situational understanding at multiple time scales, from autonomic response in the millisecond range to attack and threat scenarios over years.

References for TTA 6:

- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 5, p. 38, and Chapter 8, p. 65, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #2, p. 10, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 3, p. 124, 2007. <http://www.cyber.st.dhs.gov/documents.html>

TTA #7: Network Mapping and Measurement

a. The protection of cyber infrastructure depends on the ability to identify critical Internet resources, incorporating an understanding of geographic and topological mapping of Internet hosts and routers. A better understanding of connectivity richness among ISPs will help to identify critical infrastructure. Associated data analysis will allow better understanding of peering relationships, and will help identify infrastructure components in greatest need of protection. Improved router level maps (both logical and physical) will enhance Internet monitoring and modeling capabilities to identify threats and predict the cascading impacts of various damage scenarios.

b. Analyses related to this problem should focus on:

(1) Improving public Border Gateway Protocol (BGP) route monitoring capabilities.
(2) Extracting peering relationships from Internet topology datasets.
(3) Producing more reliable geo-location tools for visualizing and navigating geographic as well as topological connectivity.
(4) Increasing the accuracy of currently available tools for matching Internet Protocol (IPV4) addresses to router interfaces.

c. These proposed capabilities are critical to U.S. national security missions, in particular those articulated by DHS for support of DHS watch center operations, analyses of cyber infrastructure threats and risks, and hardening of U.S. military, as well as civilian, Internet communications environments. Ideally, solutions to this problem will be software-based systems that integrate multiple research areas within a common platform. A near real-time view of network maps that scale from single enterprise to the global Internet (including both logical and physical maps of critical Internet resources, either wired or wireless) is required, and research and development across multiple areas is needed, to yield sufficient operational capabilities to protect critical infrastructures dependent on the Internet.

d. This TTA will yield technologies for the protection of key infrastructure via development of, and integration between, reliable capabilities such as:

(1) Geographic mapping of Internet resources, (e.g., IPV4 or IPV6 addresses, hosts, routers, DNS servers, either wired or wireless), to GPS-compatible locations (latitude/longitude).

(2) Logically and/or physically connected maps of Internet resources (IP addresses, hosts, routers, DNS servers and possibly other wired or wireless devices).

(3) Detailed maps depicting ISP peering relationships, and matching IP address interfaces to physical routers.

(4) Monitoring and archiving of BGP route information.

(5) Development of systems achieving lasting improvement to the security and resiliency of our nation’s critical cyber infrastructure.

(6) Monitoring and measurement applied to detection and mitigation of attacks on routing infrastructure, and supporting the development and system prototype demonstration in an operational environment of secure routing protocols.

(7) Monitoring and measurement contributing to understanding of Domain Naming System (DNS) behavior, both in terms of its changing role in distributed Internet scale malware activities, such as botnets, and DNS's behavior as a system under change through DNSSEC and other potential changes affecting the root level.

References for TTA 7:

- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 8, p. 65, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Network Mapping and Measurement Conference (NMMC), 2009. <http://www.ltsnet.net/NMMC2009/index.html>
- K. Claffy, M. Fomenkov, Ethan Katz-Bassett, Robert Beverly, Beverly A. Cox, Matthew Luckie. "The Workshop on Active Internet Measurements (AIMS) Report." Appeared in ACM SIGCOMM Computer Communication Review (CCR), October 2009. Volume 39, no. 5, pp. 32-36. <http://www.caida.org/publications/papers/2009/aims_report/>
- John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett, and Joseph Bannister. "Census and Survey of the Visible Internet." In Proceedings of the ACM Internet Measurement Conference, pp. 169-182. Vouliagmeni, Greece, ACM. October, 2008. <http://www.isi.edu/~johnh/PAPERS/Heidemann08c.html>
- D. Krioukov, F. Chung, K. Claffy, M. Fomenkov, A. Vespignani, and W. Willinger. "The Workshop on Internet Topology (WIT) Report." Appeared in ACM SIGCOMM Computer Communication Review (CCR), vol.37, no.1, pp. 69-73, 2007. <http://www.caida.org/publications/papers/2007/wit/>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 4, p. 179, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." Network Mapping, p. 92, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- K. Claffy, Mark Crovella, Timur Friedman, Colleen Shannon, Neil Spring. "Community-Oriented Network Measurement Infrastructure (CONMI) Workshop Report." Appeared in ACM SIGCOMM Computer Communication Review (CCR), vol.36, no.2, pp. 41-48, 2006. <http://www.caida.org/publications/papers/2006/conmi/>
- M. Rabbat, M. Coates, and R. Nowak. "Multiple Source Internet Tomography." Appeared in Selected Areas in Communications, IEEE Journal, vol.24, no.12, pp. 2221-2234, Dec. 2006. <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4016154&tag=1>

TTA #8: Incident Response Communities

a. Cyber security incident response (CSIR) teams, individuals, and communities have historically consisted of people and organizations that have been "in the right place at the right time." Only recently has the community begun to specify the skills, abilities, structures, and support to create an effective and sustained incident response capability. While there is a good understanding of the technologies involved in CSIRTs, the operational community has not adequately studied the characteristics of individuals, teams, and communities that distinguish the great CSIR responders from the average technology contributor. In other areas where individual contributions are essential to success, e.g., first responders, commercial pilots, and military personnel, there have studies of the individual and group characteristics essential to success. To optimize the selection, training, and organization of CSIR personnel to support the essential cyber missions of DHS, a much greater understanding and appreciation of these characteristics must be achieved.

b. The proposed capabilities are critical to U.S. national security missions as the operational community addresses sophisticated attacks with cooperative and collaborative teams across the public-private partnerships that make up the U.S. CSIR infrastructure. In the context of the CSIR infrastructure, cyber incidents are expected to become more severe and involve a wider variety of infrastructure attacks than currently experienced. In particular, the expanding United States – Computer Emergency Readiness Team (US-CERT) role in the CSIR infrastructure requires that leadership within the National Cyber Security Division implement not only the appropriate technical skills, but also the individual and team characteristics that will enable an improved CSIR infrastructure.

c. The focus of research proposed under this TTA is the achievement of fundamental knowledge of the characteristics that make an excellent CSIR individual, team, and community, and how these capabilities are identified and enhanced. Research on the psychology and sociology of CSIR individuals, teams and communities should be multi-disciplinary, bringing together technologists, analysts, and social scientists to study existing and proposed CSIR individuals, teams, and communities in the course of average and extraordinary cyber response scenarios.

d. Some of the questions to be addressed by this research are:

(1) What are the most effective background experiences for an effective CSIR individual?

(2) What are the key types of individuals that currently participate in the CSIR community and which are more effective at resolving incidents?

(3) What team and organizational structures are effective and handling the current and expected range of cyber security events?

(4) What are the most effective trust models for sharing incident information between CSIR organizations, and how can these trust models be instilled in the CSIR community?

(5) What kind of work environment is most effective for CSIR individuals and teams?

(6) What user interfaces and tools are best for responders?

(7) How and where are shared communications effective?

(8) How can information overload be controlled to assure the key information is brought to the attention of the CSIR individual or team?

(9) What collection of personality types makes the most effective teams?

(10) What kind of information processors are these CSIR individuals?

(11) For the community of responders: Who are they and where do you find them? Where are they positioned in their organizations? Where do they hang out? What do they read? How can they be engaged and stitched into a national response team?

(12) Are there gaps in our national set of responders? Are there places where additional CSIR resources are needed? How would the operational community best engage them as partners in National Response Framework?

e. Proposals that offer fact-based answers to these questions will be considered. In particular, studies of CSIR team dynamics, individual attributes for CSIR individuals and teams under stress, and effective CSIR community strategies are encouraged. Lessons learned from related fields should be leveraged and expanded to form definitive understanding of the hiring, training, and organizational approaches to cyber response management.

References for TTA 8:

- GAO-08-588, Report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives; CYBER ANALYSIS AND WARNING; DHS Faces Challenges in Establishing a Comprehensive National Capability, July 2008. http://democrats.science.house.gov/Media/file/Reports/GAO_report_7.08.pdf

Introduction to TTAs #9 through #13

The Comprehensive National Cybersecurity Initiative (CNCI)
and the National Cyber Leap Year (NCLY)

a. On January 8, 2008, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 formalized the Comprehensive National Cybersecurity Initiative (CNCI) and a series of continuous efforts designed to establish a frontline defense (reducing current vulnerabilities and preventing intrusions), defending against the full spectrum of threats by using intelligence and strengthening supply chain security, and shaping the future environment by enhancing our research, development, and education, as well as investing in "leap-ahead" technologies.

b. No single federal agency "owns" the issue of cybersecurity. In fact, the federal government does not uniquely own cybersecurity. It is a national and global challenge with far-reaching consequences that requires a cooperative, comprehensive effort across the public and private sectors. Thus, as it has done historically, the U.S. Government R&D community, working in close cooperation with private-sector partners in key technology areas, can jump-start the necessary fundamental technical transformation our nation requires.

c. The Comprehensive National Cyber Initiative (CNCI) and the President's Cyberspace Policy Review challenged the federal networks and IT research community to figure out how to "change the game" to address these technical issues. Since the 2009 National Cyber Leap Year (NCLY) Summit and a wide range of other activities, the government research community has sought to elicit the best ideas from the research and technology community. The vision of the CNCI research community over the next 10 years is to "transform the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances."

d. The leap-ahead strategy aligns with the consensus of the nation's networking and cybersecurity research communities: The only long-term solution to the vulnerabilities of today's networking and information technologies is to ensure that future generations of these technologies are designed with security built in from the ground up. Federal agencies with mission-critical needs for increased cybersecurity, which includes information assurance as well as network and system security, can play a direct role in determining research priorities and assessing emerging technology prototypes.

e. The NCLY effort has proceeded on the premise that, while some progress on cybersecurity will be made by finding better solutions for today's problems, some of those problems may prove to be too difficult. The NLCY has pursued a complementary approach: a search for ways to avoid having to solve the intractable problems.
During the Leap Year, via a Request for Information (RFI) process coordinated by the Networking and Information Technology Research and Development (NITRD) Program, the technical community had an opportunity to submit ideas. The 238 RFI responses that were submitted were synthesized by the NITRD Senior Steering Group for Cybersecurity R&D and five technical areas (listed below) were identified. These areas were chosen both because the change shifts our focus to new problems, and because there appear to be technologies and/or business cases on the horizon that would promote change.
These five areas are listed below in alphabetic order, not in order of importance, as all are equally important:

(1) Cyber Economics
(2) Digital Provenance
(3) Hardware-Enabled Trust
(4) Moving-Target Defense
(5) Nature-inspired Cyber Health

f. Technical Topic Areas #9 through #13 provide the technical requirements as determined through the CNCI NCLY process and those areas of interest for DHS S&T.

References for the Comprehensive National Cybersecurity Initiative (CNCI) and the National Cyber Leap Year (NCLY) :

- "Co-Chairs' Report." Proceedings from National Cyber Leap Year Summit 2009. <http://www.cyber.st.dhs.gov/documents.html>
- "Participants' Ideas Report." Proceeding from National Cyber Leap Year Summit 2009. <http://www.nitrd.gov/NCLYSummit.aspx>

TTA #9: Cyber Economics

a. Today cyber crime pays. So does cyber-espionage. The state of cyber security today is, and in the future will be, significantly affected by economic conditions and factors. Cyber crime and espionage are making their own economic markets today, having gone well beyond the "script kiddie" and "hacker" personas to mature into big business on a global level. Gaining an understanding of the incentive structure is key to getting stakeholders to behave in a way that will improve overall security. Current cyber-related illegal activities are economically attractive for several reasons:

(1) Cost to engage in them is very small compared to the return on investment.

(2) Attack development costs can be amortized over both time and space.

(3) Cyber resources upon which the illicit activities are built are cheap, even free, thanks to resources such as webmail and botnets.

(4) Risk of being caught or exposed (law enforcement) is low relative to potential payoffs, given that many attacks are carried out using other people's assets.

b. This TTA seeks to promote the role of economics in identifying and realigning cyber economic incentives by creating science-based understanding of markets, decision making, and motivators; promote an environment where system prototype demonstration in an operational environment of security technology is balanced, providing incentives to engage in socially responsible behavior and deter those who participate in criminal and malicious behavior. As an emerging field, cybersecurity economics describes a range of areas that are not well understood in linking economic factors with cyber security. These research challenges are multi-disciplinary in nature, combining engineering, computer science, business, economics, and behavioral and social sciences.

c. The economics of cybersecurity reflects the recognition that information security problems are, fundamentally, issues of misaligned incentives and misallocated resources and, therefore, economic problems that require economic, more than merely technical, solutions. Accordingly, the Cyber-Economics group at the 2009 National Cyber Leap Year (NCLY) Summit identified four economic strategies through which research and policy efforts may spur changes in cybersecurity:

(1) **Mitigating incomplete information**: Mitigate incomplete and asymmetric information barriers that hamper efficient security decision-making at the individual and organizational levels.

(2) Incentives and liabilities: Leverage incentives and impose or redistribute liabilities to promote secure behavior and decision making among stakeholders.

(3) Reducing attackers' profitability: Promote legal, technical, and social changes that reduce attackers' revenues or increase their costs, thus lowering the overall profitability (and attractiveness) of cybercrime.

(4) **Market enforceability**: Ensure that proposed changes are enforceable with market mechanisms.

d. In addition to the above four directions, the NCLY Cyber Economics group observed that the purpose of information and communication technologies is not to provide perfect security, but to enable society to accomplish other objectives. This implies that the R&D community should not focus on absolute but on relative concepts of security and reliability in an unavoidably, necessarily insecure world; a fundamental issue of costs and benefits.

e. Also, secure practices must be incentivized if cybersecurity is to become ubiquitous, and sound economic incentives need to be based on sound metrics (see TTA #2), on processes that enable assured development, on sensible and enforceable notions of liability and on mature cost/risk analysis methods. Without a scientific framework, it is difficult to incentivize good cybersecurity practices and subsequently to make a convincing business case for enhanced cybersecurity mechanisms or processes. The benefits must be quantified to demonstrate they outweigh the costs incurred by the implementation of improved cybersecurity measures. There is no scientific basis for cost/risk analysis and business decisions are often based on anecdotes or unquantified arguments of goodness. Currently, it is also very difficult to collect the large body of data needed to develop a good statistical understanding of cyberspace without compromising the privacy of individuals or the reputation of companies. The means to identify and realign cyber economic incentives and to provide a science-based understanding of markets, decision making, and motivators must be investigated.

f. Research areas include: understanding risks, incentives, disincentives, and value-chains; aligning stakeholders interests through market-driven approaches; understanding return on investment from malicious activities, in quantity and methodology, and how to diminish those returns; understanding how to economically incentivize stronger cyber security postures at the individual, enterprise, and national levels in private and public arenas; understanding and measuring the cost of cyber security practices to productivity; and understanding and measuring the cost of security breaches and the benefits of security protections.

g. The results of the National Cyber Leap Year (NCLY) Summit categorized the current needs into 13 areas for consideration. For this TTA, DHS S&T is interested in proposals that respond to the following topic areas:

(1) Develop new theories and models of cyber economics and scientific understanding of the social dimensions of cyber economics.

(2) Develop scientific frameworks to incentivize vendors of cyberspace-related technologies e.g., encourage use of secure software engineering and analysis practices, software vulnerability detection, security incident forensics) through acquisition, regulation, and standards.

(3) Promote an environment where (1) users are well informed about cyber security; and, (2) individuals have “ownership” of their personal data, are aware of its provenance, and control its authenticated and authorized distribution, use, destruction with improved understanding of the economic value of such data.

(4) Empower cyberspace service providers e.g., Internet Service Providers, Application Service Providers, registrars, registries, banks, countries, nation-states, etc., to reduce abusive or criminal

behavior and to provide the means to better defend services and systems against abuses and exploitation, while offering the appropriate legal/regulatory framework e.g., exemptions, liability protection, and law enforcement support.

h. In addition to the topic areas listed above, the following categories are worthy of exploration and valid directions for this TTA:

(1) Studying how to inject costs as disincentives to criminal behavior.

(2) Evaluating economic policies to strengthen our cyber security posture.

(3) Exploring issues of insurability against cyber attacks that can lead to policies and standards.

(4) Studying the economic impact of cyber security recommendations that affect the efficiency or effectiveness of critical national resources.

(5) Developing models to determine what the appropriate level of investment is for the criticality of assets and information.

(6) Understanding the economic cost-benefit of protecting critical infrastructure against disruption through cyberspace means, and educate vendors about their role in protecting critical infrastructure and consequences of failures in this domain.

(7) Determining the scope of action allowed by service providers and the boundaries between service provider empowerment and law enforcement involvement, within the context of their global legal abilities and partnerships.

(8) Analyze current models of cybersecurity investment and usage to determine future economic drivers.

(9) Examining the legal and technical issues and barriers involved in data sharing among service providers, both domestic and global, and developing improved models for domestic and international collaboration and data sharing.

References for TTA #9:

- "Co-Chairs' Report ." Proceedings from National Cyber Leap Year Summit 2009, pp. 46-57, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- "Participants' Ideas Report." Proceeding from National Cyber Leap Year Summit 2009, pp. 75-85, 2009. <http://www.nitrd.gov/NCLYSummit.aspx>
- Workshops on the Economics of Information Security (WEIS), 2002-2009. Most recent - <http://weis09.infosecon.net/past_workshops.html>
- "Cybersecurity Economic Issues: Corporate Approaches and Challenges to Decisionmaking." In RAND research brief, 2008. <http://www.rand.org/pubs/research_briefs/RB9365-1>
- "National Cyber Security: Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior." In I3P report for the United States Senate, February 2009. <http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf>
- "The Economics of Cybersecurity." In I3P Research Report. <http://www.thei3p.org/docs/publications/138.pdf >

TTA #10: Digital Provenance

a. Individuals and organizations routinely work with, and make decisions based on, data that may have originated from many different sources and also may have been processed, transformed, interpreted, and aggregated by numerous entities between the original sources and the consumers. Without good knowledge about the sources and intermediate processors of the data, it can be difficult to assess the data's trustworthiness and reliability, and hence its real value to the decision-making processes in which it is used.

b. Physical provenance markings in jewelry, e.g., claiming your diamond is from a blood-free mining operation, your silver or gold is pure, and the style is not a knockoff copy of a designer's, explosive components, e.g., nitrates, and clothing have historically added value and enabled tracing of origin. Document markings such as wax seals and signatures have been used to increase assurance of authenticity of high-value documents for centuries. More recently the legal, auditing, and medical fields have begun to employ first-level authenticated provenance markings.

c. Digital Provenance refers to the chain of successive custody, including sources and operations, of computer-related resources such as hardware, software, documents, databases, data, and other entities. Provenance includes pedigree, which relates to the total directed graph of historical dependencies. It also includes tracking, which refers to the maintenance of distribution and usage information that enables determination of where resources went and how the resources may have been used. Identity is a unique reference to a distinct (possibly composite) entity. It is a recursive concept based on the context; any attribute of an entity may be considered an identity. Digital provenance of an object is the set of identities, labels, and events associated with the object.

d. Provenance is also concerned with the original sources of any subsequent changes or other treatment of information and resources throughout the life cycle of data. That information may be in any form, including software, text, spreadsheets, images, audio, video, proprietary document formats, databases, and others, as well as metalevel information about information and information transformations, including editing, other forms of markup, summarization, analysis, transformations from one medium to another, formatting, and provenance markings. Provenance is generally concerned with the integrity and reliability of the information and meta-information rather than just the information content of the document.

e. Provenance can also be used to follow modifications of information, for example, providing a record of how a document was derived from other sources or providing the pervasive history through successive versions (as in the Concurrent Versions System [CVS]), transformations of content (such as natural language translation and file compression, and changes of format (such as Word to .pdf).

f. DHS S&T envisions an end state in which digital provenance enables identification, authentication, and reputation for entities and objects with appropriate granularity at many layers. For example, networked entities will be capable of authenticating the origin(s) and integrity of communications traffic. Also, digital provenance will enable users to identify and authenticate the origins of data objects. This can help mitigate spoofing, phishing, denial of service (DoS), and impersonation attacks.

g. The granularity of provenance ranges from whole systems through multi-level security, file, paragraph, and line, and even to bit. For certain applications, such as access control, the provenance of a single bit may be very important. Provenance itself may require meta-provenance, that is, provenance markings on the provenance information. The level of assurance provided by information provenance systems may be graded and lead to graded responses. Note that in some cases provenance information may be more sensitive, or more highly classified, than the underlying data. The policies for handling provenance information are complex and differ for different applications and granularities. Note that situations are likely to arise where absence of provenance is important—for example, where information that needs to be made public must not be attributable.

h. In addition, new techniques are needed that will allow management of provenance for voluminous data. Part of what has made provenance easier to manage up to now is its small volume. Now, geospatial information-gathering systems are being planned that will have the capability of handling gigabytes of data per second, and the challenges of these data volumes will be exacerbated by collection via countless other sensor networks. Within 20 years, the government will hold an exabyte of potentially sensitive data. The systems for handling and establishing provenance of such volumes of information must function autonomously and efficiently with information sources at these scales.

i. The current practice is rather rudimentary compared with what is needed to be able to routinely depend on provenance collection and maintenance. The financial sector, in part driven by Sarbanes-Oxley requirements, has developed techniques to enable tracking of origins, aggregations, and edits of data sets. Users of document production software may be familiar with change-tracking features that provide a form of provenance, although one that cannot necessarily be considered trustworthy.

j. Numerous gaps in provenance and tracking research remain to be filled, requiring a much broader view of the problem space and cross-disciplinary efforts to capture unifying themes and advance the state of the art for the benefit of all communities interested in digital provenance.

k. Provenance may be usefully subdivided along three main categories, each of which may be further subdivided, as follows:

(1) **Representation**: data models and representation structures for provenance (granularity and access control).

(2) **Management** (creation; access; annotation [mark original documents/resources with provenance metadata]; editing [provenance-mark specific fine-grained changes through the life cycle]; pruning [delete provenance metadata for performance, security, and privacy reasons]assurance; and revocation).

(3) **Presentation** (query [request provenance information]; present [display provenance markings]; alert [notify when provenance absence, compromise, or fraud is detected).

l. Information provenance presents a large set of challenges, but significant impact may be made with relatively modest technical progress. For example, it may be possible to develop a coarse-grain information provenance appliance that marks documents traversing an intranet or resting in a data center and makes those markings available to decision makers. Although this imagined appliance may not have

visibility into all the inputs used to create a document, it could provide relatively strong assurances about certain aspects of the provenance of the information in question. It is important to find methods to enable incremental rollout of provenance tools and tags in order to maintain compliance with existing practices and standards. Another incremental view is to consider provenance as a static type system for data. Static type systems exist for many programming languages and frameworks that help prevent runtime errors. By analogy, it may be possible to create an information provenance system that is able to prevent certain types of misuse of data by comparing the provenance information with policies or requirements.

m. The results of the National Cyber Leap Year (NCLY) Summit categorized the current needs into 8 areas for consideration. For this TTA, DHS S&T is interested in proposals that respond to the following two topic areas:

(1) Data Provenance Security; refer to NCLY Participants Report section 3.2.
(2) Data Provenance Definition and Management; refer to NCLY Participants Report section 3.3.

n. Digital provenance is at the core of many of our problems today and solutions are needed in the areas listed above to move us forward. It is important to find methods to enable incremental rollout of provenance tools and techniques in order to maintain compliance with existing practices and standards.

References for TTA #10:

- "Co-Chairs' Report ." Proceedings from National Cyber Leap Year Summit 2009, pp. 46-57, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- "Participants' Ideas Report." Proceeding from National Cyber Leap Year Summit 2009, pp. 75-85, 2009. <http://www.nitrd.gov/NCLYSummit.aspx>
- DHS Science and Technology. "A Roadmap for Cybersecurity Research." Chapter 9, p. 76, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. "Research Agenda for the Banking and Finance Sector." Challenge #5, p. 17, 2008. <http://www.cyber.st.dhs.gov/documents.html>
- National Research Council. "Toward a Safer and More Secure Cyberspace." Category 2, p. 113, 2007. <http://www.cyber.st.dhs.gov/documents.html>
- National Science and Technology Council. "Federal Plan for Cyber Security and Information Assurance Research and Development." p. 75, 2006. <http://www.cyber.st.dhs.gov/documents.html>
- INFOSEC Research Council. "Hard Problems List." Problem #6 – Information Provenance, p. 25, 2005. <http://www.cyber.st.dhs.gov/documents.html>
- L. Moreau, J. Freire, J. Futrelle, R. E. McGrath, J. Myers, and P. Paulson. "The Open Provenance Model." Technical report, ECS, University of Southampton, 2007. <http://eprints.ecs.soton.ac.uk/14979/>
- First Workshop on the Theory and Practice of Provenance. San Francisco, February 23, 2009. <http://www.usenix.org/events/tapp09/>
- Sarbanes-Oxley Act of 2002, Pub. L no. 107-204, 115 Stat 2390.

TTA #11: Hardware-Enabled Trust

a. Hardware can be the final sanctuary and foundation of trust in the computing environment, based on the technologies that can be developed in the area of hardware-enabled trust and security. With cyber threats steadily increasing in sophistication, hardware can provide a game-changing foundation upon which to build tomorrow's cyber infrastructure. But today's hardware still provides limited support for security and capabilities that do exist are often not fully utilized by software. The hardware of the future also must exhibit greater resilience to function effectively under attack.

b. Continually increasing transistor densities have ushered in an era of multi-core microprocessors and increasing computing power in embedded processors. This has dramatically reduced the cost of hardware support for trust and security. At the same time, the increasingly pervasive nature of networked computing devices in our digital society has made trust in these devices and the environment where they operate more critical than ever. This pivotal balance between cost and benefit suggests that a tipping point is at hand, security will be increasingly demanded throughout the global computing system. Industry must be prepared to provide security based on new developments in hardware-related research.

c. The strategies presented at the National Cyber Leap Year (NCLY) Summit are game-changing because they do not assume a perfect world. Rather, these strategies assume all software is vulnerable to attacks, and even hardware/physical attacks are likely with the billions of diverse mobile computing and communications devices that can be lost or stolen. However, our computing devices, not only the datacenters, networks, or cloud servers, will be designed from hardware on up, to provide intrinsic security. Attendees believe the role of hardware in establishing a safer computing environment will grow. This is a change from predominantly software security solutions. Hardware security solutions will be harder to break, increasing the "work factor" for attackers and, therefore, serving as an additional deterrent. Hardware computer and device architecture will provide fundamental features to enable us to build more trustworthy software and systems, and hardware itself will be built to be more trustworthy. For example, new technologies will ensure that hardware will not inadvertently leak secrets or execute malware (even if penetrated by malware), and it will execute security-critical tasks even if partially compromised. With enhanced research activity in this area, basic security mechanisms will be seamlessly provided without impacting the performance, energy consumption, cost, and usability of commodity computers and on-line services. Moreover, intrinsically secure computing devices will be able to share provable trust information, confirming their trustworthiness.

d. The NCLY Summit identified three very promising hardware-related technology strategies:

(1) End-to-End Trust; refer to NCLY Co-Chairs Report section 2.2.
(2) Enabling Hardware to Thwart Attacks; refer to NCLY Co-Chairs Report sections 2.3-2.5.
(3) Hardware-enabled Resilience; refer to NCLY Co-Chairs Report section 2.6.

e. **End-to-End Trust.**

(1) The NCLY Summit attendees define "end-to-end trust" as the ability to secure trust in a distributed heterogeneous environment. Technologies discussed in this section are hardware-based or hardware-enabled. End-to-end trust is a collection of technologies, behaviors, implementations, and infrastructure approaches that, when used consistently, can enable a predictable level of trust in the entire system. The key to building end-to-end trust lies in identifying "trust properties" that can be used to determine the state of health of the system. For a device, these properties can include evidence of the authenticity of the hardware, proof that the devices and its software has not been compromised, and

other general or domain specific "trust" information. In addition, there is a need for protocols to exchange this evidence of "trust" information, approaches to dynamic measurement of the health of the system, and a way to compose and evaluate the resulting "trust messages" in order to make a determination of the trustworthiness of a device.

(2) Currently, devices and networks contain some information about their trustworthiness that helps them operate in their operational environment. Examples of such information include the fact that a mobile phone ID has not been blacklisted, e.g., because the device was stolen, as a condition of connecting to a mobile network; evidence of up-to-date security patching when connecting to a corporate network, or comparisons of configuration measurements obtained at run time with those stored in a Trusted Platform Module (TPM). This information, however, is not sufficient to evaluate the trust state of a device or network, and is expressed and transmitted in terms and via protocols that are not interoperable. For example, when exchanging security-critical messages between a smart phone and a PC, each device currently has limited ability to determine the trustworthy state of the other and to communicate it.

(3) Ensuring that all communicating devices are trustworthy and operate in a trustworthy environment (that is, if it were possible to establish end-to-end trust), the computing environment would be safer because each entity participating in a transaction could either vouch for its "trustworthy" state, or refuse to participate in a transaction without obtaining evidence of remediation. In order to achieve this, there is a need for a foundation of interoperability across devices, systems and networks. Our vision is of a future where each device, from a sensor to a PC or server, and each network can be trusted based on a set of hardware-enabled "trust attributes" that could be exchanged over common protocols using appropriate trusted infrastructure.

(4) The limited ability to establish and communicate trust that exists in generic devices and platforms is not sufficient to provide adequate levels of assurance across the computing environment. When determining a system's level of trust, some questions can be formulated reflecting the main areas of concern:

(a) Is the system secure (does it have the expected security properties and configuration)?

(b) Is it in good standing (did it sustain attacks or unauthorized modifications)?

(c) Is it trustworthy (can it be trusted for the types of tasks it is expected to perform)? Even if "broken" in the future, can past operations be trusted?

(d) Is the system genuine (does it comprise only authentic components that are correctly implemented and are those parts assembled in a genuine way for both hardware and software)?

(e) What was its path from manufacturing to system prototype demonstration in an operational environment?

(f) Was the design of its elements compliant with the best industry and technology practices?

(5) If technology were available that could dynamically answer most of these questions in an automated fashion for all components of the system, the state of security assurance would be more on par with the dynamic nature of today's computing environment. Thus, NCLY Summit attendees think that innovation could be introduced by focusing on the following activities:

(a) Define a canonical set of security and trust properties supplemented by domain-specific information. These properties will attest to the trusted state of a device or system, will be available dynamically to help discover trustworthy resources, and will be rooted in hardware.

(b) Design protocols to communicate this dynamic trust information.

(c) Create infrastructure to verify and transmit this trust information.

(d) Develop processes to compose elements of this information into evidence or a "trust message" and evaluate it.

(e) Identify approaches to support dynamic measurement of relevant parameters to ensure trust information is refreshed as appropriate.

(f) Demonstrate interoperability to support this functionality across various operational scenarios.

(g) Ideally, devices will be able to exchange trust messages prior to accepting connections or messages. Finally, in terms of system development, it would be attractive to build systems from the bottom up with constraints that can enforce safer behavior at all levels. Hierarchical trust models that are currently used in most systems have multiple dependencies (software needs to trust other software and operating systems). It would be interesting and productive to consider replacing these models with a new generation of trust models rooted in hardware.

f. **Enabling Hardware to Thwart Attacks.**

(1) Today, system owners do not know whether there is malware in their computers and also cannot prevent inadvertent information leakage from our correctly-executing hardware. Tomorrow, our vision is to design computers that will **not** execute malware. Our personal computing devices will enable us to control the protection of our private information stored in on-line storage systems, and will not leak information through side-channel attacks.

(2) NCLY Summit attendees propose three major directions for hardware to counter attacks:

(a) Trustworthy hardware that will not leak information.
(b) Hardware that will not execute malware.
(c) Hardware-assisted secure storage and self-protecting data.

g. **Trustworthy hardware that will not leak information.**

(1) Today, attackers can obtain secret or sensitive information from our computers by side-channel attacks without breaking any rules or security policies, but just by observing hardware behavior. This undermines strong cryptographic protections and strong software isolation provided by VM technology.

(2) Tomorrow, it is imperative that there are computers that have leak-free hardware, where trustworthy hardware components and systems do not leak information. Only very slow or inaccurate side-channel attacks would be possible - hence, significantly increasing the work factor for the attacker and changing the game.

h. **Hardware that will not execute Malware.** Today, hardware blindly executes any software, including malware. Tomorrow, the game change proposed is that even if the computer is penetrated by malware, this malware will not be executed. This assumes an imperfect world where malware can exist in a computer but do no damage, just as viruses may exist in a healthy human body but not cause illness.

Hardware will be designed to continuously measure and monitor normal behavior, and thus thwart the execution of many types of malware. Hardware will be designed to instinctively protect overuse of its resources, or other actions that damage the health and welfare of the system. In this regard, there is synergy between this research thrust and Nature-inspired Cyber Health (TTA #13).

i. **Hardware-assisted secure storage and self-protecting data.** Today, users are concerned about storing their secret or sensitive information in on-line storage, e.g., in Cloud storage. Privacy concerns prevent consumers from storing sensitive data, and confidentiality concerns prevent companies from storing proprietary information. Our vision is to develop user-controlled secure storage technologies that prevent adversaries from being able to view or modify such data, which could be stored in essentially un-trusted storage and transmitted over public networks. Of course, the Cloud storage provider should also make every attempt to provide secure and reliable on-line storage. In the longer term, there is a need for new architectures for self-protecting data, which can essentially be stored anywhere.

j. **Hardware-Enabled Resilience.**

(1) Today, a compromised system does not guarantee the integrity or availability of critical services. Tomorrow, there is a need for resilient computer hardware that can guarantee the execution of critical services even while compromised. This will significantly increase the work factor of attackers by protecting critical services from corruption or denial of service. Today, if a system has been compromised, there is no easy way to get back to a pristine state. Tomorrow, the hardware (together with trusted software) will restore this pristine state.

(2) NCLY Summit attendees envision future systems that provide these guarantees by leveraging techniques traditionally applied to achieve fault tolerance and apply these techniques to protect critical services from attack. This game change could be a key enabler for a future Internet immune from malware disruption.

(3) Specifically, NCLY Summit attendees envision future systems that incorporate the following techniques in hardware: redundancy, diversity, check-pointing and recovery, and self-repair and evolution.

References for TTA 11:

- "Co-Chairs' Report." Proceedings from National Cyber Leap Year Summit 2009, pp. 8-24, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- "Participants' Ideas Report." Proceeding from National Cyber Leap Year Summit 2009, pp. 86-99, 2009. <http://www.nitrd.gov/NCLYSummit.aspx>

TTA #12: Moving-Target Defense

a. In the current environment, our systems are built to operate in a relatively static configuration. For example, addresses, names, software stacks, networks, and various configuration parameters remain relatively static over relatively long periods of time. This static approach is a legacy of information technology system design for simplicity in a time when malicious exploitation of system vulnerabilities was not a concern.

b. In order to be effective, adversaries must know a particular vulnerability of a system. The longer the vulnerability of a system exists, the more likely it is to be discovered and then exploited. Many system vulnerabilities are published by researchers and software vendors in order for system owners to patch those vulnerabilities. A system that remains unpatched is vulnerable to exploitation. Vulnerabilities that are not publicly disclosed are called zero-day vulnerabilities, and are known to a limited set of people. Zero-day vulnerabilities present a large risk to system owners because without knowledge of the vulnerability, system owners have no way to patch it.

c. It is now clear that static systems present a substantial advantage to attackers. Attackers can observe the operation of key IT systems over long periods of time and plan attacks at their leisure, having mapped out an inventory of assets, vulnerabilities, and exploits. Additionally, attackers can anticipate likely responses and deploy attacks that escalate in sophistication as defenders deploy better defenses. Attackers can afford to invest significant resources in developing attacks since the attacks can often be used repeatedly from one system to another.

d. Current approaches to addressing this problem are to remove bugs from software at the source, patch software as rapidly and uniformly as possible, and identify malicious attacks against soft-ware. The first approach of perfect software development does not scale to complete protection because the complexity of software precludes perfection. The second approach of patch distribution is now standard practice in large enterprises and has proven difficult to keep ahead of the threat. It also does not provide protection against zero-day attacks. The last approach is predicated on having a signature or definition of the malicious attack in order to find it and potentially block it. However, the speed and agility of adversaries as well as simple polymorphic mechanisms that continuously change the signatures of attacks renders signature-based approaches largely ineffective.

e. The magnitude of this problem suggests that information technology community needs a radically new approach for IT system defense. To visualize the elements of the new environment, observe that for attackers to exploit a system today, they must learn about a vulnerability and hope that it is present long enough to exploit. For defenders to defeat attacks today, they must develop a signature of malware or attacks and hope it is static long enough to block that attack. Malware writers develop mechanisms to rapidly change malware in order to defeat detection mechanisms. We, as defenders, should learn from this approach, and build systems that rapidly change, never allowing the exploitation of a particular vulnerability to impair the ability of a system to perform its mission/function, or if exploited once, not allowed to be exploitable again. If done correctly, this “moving target" defense can present a formidable obstacle to attackers since attackers depend on knowing a system's vulnerabilities a priori.

f. Therefore, a game-changing approach to building self-defending systems can and must be developed. Protecting systems (thus avoiding exposed vulnerabilities) to the greatest extent possible should still be the first goal. However, recognizing that absolute perfection in software or hardware is untenable, the NCLY Summit attendees proposed an alternate strategy that continuously shifts the attack surface of the system.

g. This new approach is known as, "Moving Target Defense (MTD)." An important benefit of moving target defense is to decrease the known attack surface area of our systems to adversaries while simultaneously shifting it; a key challenge of moving target defense is to ensure that our systems remain dependable to their users and maintainable by their owners. By making the attack surface of software appear chaotic to adversaries, it forces them to significantly increase the work effort to exploit vulnerabilities for every desired target. For instance, by the time an adversary discovers a vulnerability in a service, the service will have changed its attack surface area so that an-other exploit against that vulnerability will be ineffective.

h. Research into moving target defense technologies will enable us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency. The characteristics of a MTD system are dynamically changed in ways that are manageable by the defender yet make the attack space appear unpredictable to the attacker. Moving target defense technology changes the game by wresting the advantage from the attacker because it eliminates the availability of constant or slowly-changing vulnerability windows that allow attackers to lie in wait and conduct useful experiments on persistent vulnerabilities.

i. This game-changing approach challenges the traditional approach which councils that adding complexity to our systems adds risk. Conversely, the complexity of today's compute platforms and analytic and control methods can now be used to frustrate our adversaries. The challenge is to demonstrate that complexity is indeed a benefit and not a liability.

j. The results of the National Cyber Leap Year (NCLY) Summit categorized the current needs into research areas for consideration as follows:

(1) Develop abstractions and methods that will enable scientific reasoning regarding MTD mechanisms and their effectiveness.

(2) Characterize the vulnerability space and understand the effect of system randomization on the ability to exploit those vulnerabilities.

(3) Understand the effect of randomization of individual components on the behavior of complex systems, with respect to both their resiliency and their ability to evade threats.

(4) Develop a control mechanism that can abstract the complexity of MTD systems and enable sound, resilient system management.

(5) Enable the adaptation of MTD mechanisms as the understanding of system behavior matures and our threat evolves.

k. The MTD area has its underpinnings in fundamental research in the following supporting or component areas: virtualization, multi-core processing, new networking standards, cryptography, system management, software application development, and evolutionary resiliency and defense methods.

l. For this TTA, DHS S&T is interested in proposals that respond to the five topic areas listed above as well as all of the areas of underpinning fundamental research mentioned above.

References for TTA #12:

- "Co-Chairs' Report ." Proceedings from National Cyber Leap Year Summit 2009, pp. 46-57, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- "Participants' Ideas Report." Proceeding from National Cyber Leap Year Summit 2009, pp. 75-85, 2009. <http://www.nitrd.gov/NCLYSummit.aspx>

TTA #13: Nature-Inspired Cyber Health

a. Today, weeks and months may elapse before successful network penetrations are detected through laborious forensic analysis. Despite their potential to function with intelligence, today's typical network components have very limited understanding of what passes through them, coupled with a correspondingly short memory. In the future, network components must have heightened ability to observe and record what is happening to and around them. With this new awareness of the system health and safety, these "self-aware systems" enjoy a range of options: these system may take preventative measures, rejecting requests which do not fit the profile of what is good, *a priori*, for the network; these systems can build immunological responses to the malicious agents which they sense in real time; these systems may refine the evidence they capture for the pathologist, as a diagnosis of last resort, or to support the development of new prevention methods. In the future, system owners should be able to monitor and control such dynamic cyber environments.

b. This TTA is interested in looking to nature for inspiration. As part of the NCLY, one study group focused on nature-inspired approaches to cybersecurity. Given one of the best ways to generate novel ideas is to look to natural systems for inspiration, these systems evolved to face specific threats and have undergone millions of year of evolutionary selection to select the best fit. Examples in nature are the immune system, beneficial parasites, and social networks such as public health networks and social insects. The biological immune system consists of many organisms used to defend against invaders. Such systems function remarkably well in distributed, complex and ever-changing environments, even when subject to a continuous barrage of attacks. Natural systems are far more complex than our cyber-systems but they are extremely robust, resilient, and effective. Clearly, an investigation of these natural systems, such as the immune system, can be beneficial to changing the landscape for cyber-security.

c. The R&D community has only just begun to mine the wealth of possibilities provided by the correspondence between biological immunity and cybersecurity. There is much to learn and much to potentially gain. The NCLY Summit attendees continue to believe that the Biological Immune System (BIS) is one of the best existing examples of an effective defense mechanism for a complex system that could yield new insights that could be make a difference for cybersecurity. The BIS is a robust defense system that has evolved in vertebrates to protect them from invading pathogens. To accomplish its tasks, the BIS uses sophisticated detection and response mechanisms and follows differential response pathways, i.e., depending on the type of pathogen, the way it enters the body and the damage it causes, the immune system uses various mechanisms for detection, recognition and subsequent destruction of the invader or neutralization of its effects. In medicine, historically, the term immunity refers to the condition in which an organism can resist disease, more specifically infectious disease. However, a broader definition of immunity is a reaction to foreign (or dangerous) substances. Cells and molecules responsible for immunity constitute the BIS, and the collective coordinated response of such cells and molecules in the presence of pathogens, is known as the immune response. The BIS can be envisioned as a multilayer protection system, where each layer provides different types of defense mechanisms. For example, skin and mucus membranes provide the first level of defense by blocking/filtering out many bacteria, fungi, etc. There are three (3) main layers which include the anatomic barrier, innate immunity (nonspecific) and adaptive (specific) immunity. Innate (non-specific) immunity and adaptive (specific) immunity are inter-linked and influence each other. Once adaptive immunity recognizes the presence of an invader, it triggers two types of responses: humoral immunity and cell-mediated (cellular) immunity, which act in a sequential fashion. Innate immunity is usually directed against an invading pathogen;

however, if the pathogen evades the innate defenses, the body launches an adaptive and specific response against it. Signaling is essential for activating and coordinating biological defenses. Signaling also allows a cell to transfer information about its internal state to its environment, where it can be recognized by cells in the Immune system. Furthermore, signaling results in changes to the cell, allowing it to appropriately respond to a stimulus.

d. From an information-processing perspective, there are several immunological principles that make the system very appealing, which include distributed processing, pathogenic pattern recognition, multi-layered protection, decentralized control, and diversity and signaling.

e. Understanding the immune mechanisms on the abstract level could result in the development of novel approaches to solve problems of cybersecurity: early and dependable detection and recognition of information attacks, rational utilization of the network resources for minimization of the damage and fast recovery, and development of successful ways to prevent further attacks.

f. The compelling similarities between the problems facing the community in cybersecurity and those faced by biological systems have sparked investigative research to analyze how biological immunology concepts can be applied to cybersecurity. Immuno-computing or Artificial Immune Systems (AIS) emerged in the 1990s as a new computational intelligence field. For example, in 1996, an attempt was made to define the equivalent of the biological "self" for a computer system. This led to a novel approach to anomaly and intrusion detection, which spawned a new area in cybersecurity research. Ongoing research into the analogy between cybersecurity and immunology continues to result in useful ideas. The work in the references below laid the foundations for this area of research. Although most of the currently active research into cybersecurity that is inspired by nature focuses on the immune system, there are many other natural systems that could serve as inspiration for cybersecurity.

g. Another promising development is trying to understand how research could use the Danger Model concept to refine the accuracy of cybersecurity response, because not all abnormal events (non-self) represent attacks – only a small percentage of such events are of real concern. Simple observations can be used to trigger a chain of defensive actions, but the challenge is clearly to define what constitutes suitable danger signals.

h. The results of the National Cyber Leap Year (NCLY) Summit categorized the current needs into 5 areas for consideration. For this TTA, DHS S&T is interested in proposals that respond to the following topic areas aimed at exploring immunological principles to automatically detect situational changes, determine imminent danger and mitigate cyber attacks:

(1) Thwart malicious attacks through signaling, implementation of diversity and immunogenic detection as hardware-software solutions. Rapidly regenerate (self-healing) survivable capabilities in mission critical systems after an sophisticated attack.

(2) Evolve immunity to attacks through evolutionary computing to create new deceptions (gaming strategies) as new threats emerge. Self-learning while monitoring insider activity and develop profiles for appropriate and legitimate behavior (modeling).

(3) Signaling and Message-passing: Integrating the many disparate security tools using both feed forward and feedback signaling mechanisms in a cyber defense system should help to ensure tolerance and identify attacks while minimizing false alarms (i.e. improve judgments between dangerous attacks and benign anomalies).

(4) Decentralized Control: The immune system uses distributed control mechanisms for learning, memory and associative retrieval to solve recognition and classification tasks. There is no single organ that controls the immune response; rather it handles the antigenic challenges through collaborative interaction. A similar strategy (distributed control mechanisms for monitor and response) needs to be pursued as a game changing strategy in cyber defense in order to avoid a single point of failure and to enable robust decision making.

(5) Missing Self Paradigm: The missing self hypothesis from immunology literature may shed new light to secure host systems, in particular, to validate, authenticate and permit codes, data and scripts to execute in a machine. Different techniques are used to preserve integrity at the process, system and communication levels. For example, commercial solutions ensure system level integrity and security; whereas, digital signature, code signing, watermarking, integrity checker, magic cookies, etc. address file integrity of data and executables in transit.

i. DHS S&T believe that there needs to be an emphasis on the ongoing exploration of this area, especially cross-disciplinary research bringing together computer scientists, biologists and immunologists. New insights and game-changing ideas often come from the intersection of radically different research fields. This TTA seeks those new insights and ideas.

References for TTA 13:

- "Co-Chairs' Report ." Proceedings from National Cyber Leap Year Summit 2009, pp. 46-57, 2009. <http://www.cyber.st.dhs.gov/documents.html>
- "Participants' Ideas Report." Proceeding from National Cyber Leap Year Summit 2009, pp. 75-85, 2009. <http://www.nitrd.gov/NCLYSummit.aspx>
- S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff. "A sense of self for Unix processes." Appeared in Proc. of 1996 IEEE Symposium on Computer Security and Privacy, 1996. <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=502675&tag=1>
- D. Dasgupta. *Book-Immunological Computation*. CRC press, September 2008.
- P. D'haeseleer, S. Forrest, and P. Helman. "An immunological approach to change detection: algorithms, analysis, and implications." Appeared in Proc. of the 1996 IEEE Symposium on Computer Security and Privacy, IEEE Computer Society Press, Los Alamitos, CA, pp. 110-119, 1996. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=00502674>
- S. Forrest, S. Hofmeyr, and A. Somayaji. "Computer Immunology." Appeared in Communications of the ACM, Vol. 40, No. 10, pp. 88-96, 1997. <http://scholar.google.com/scholar?hl=en&q=A.+Somayaji.+Computer+Immunology&as_sdt=20000&as_ylo=&as_vis=1>
- A. Somayaji, S. Hofmeyr, and S. Forrest. "Principles of a Computer Immune System." Appeared in New Security Paradigms Workshop, pp. 75-82, 1998.

<http://scholar.google.com/scholar?q=A.+Somayaji.+Computer+Immunology&hl=en&as_sdt=0&as_vis=1&oi=scholart>

- S. A. Hofmeyr and S. Forrest. "Immunity by Design: An Artificial Immune System." Appeared in Proc. of 1999 GECCO Conference, 1999. <http://scholar.google.com/scholar?hl=en&q=S.+Forrest.+Immunity+by+Design%3A+An+Artificial+Immune+System.+&as_sdt=20000&as_ylo=&as_vis=1>
- T. S. Guzella, T. A. Mota-Santos and W. M. Caminhas. "A novel immune inspired approach to fault detection." From Lecture Notes in Computer Science, Proceedings of ICARIS, 2007. <http://www.springerlink.com/content/4232244522w554u4/>
- J. O. Kephart. "A biologically inspired immune system for computers." In R. A. Brooks and P. Maes, (Eds.), Artificial Life IV. Proceedings of the 4th International Workshop on the Synthesis and Simulation of Living Systems, MIT Press, Cambridge, MA, pp. 130–139, 1994. <https://researcher.ibm.com/researcher/view_pubs.php?person=us-kephart>

TTA #14: Software Assurance MarketPlace (SWAMP)

a. Technical Topic Area #1 on Software Assurance describes the need to address threats throughout the software development process and called for new methods, services, and capabilities in build, test, and analysis phases in order to improve the quality and reliability of software used in the nation's critical infrastructures. Specifically, TTA#1 solicits ideas for research and development of new tools and methods for software analysis, and for applying new and existing capabilities in test and evaluation activities. This TTA (#14) focuses on the research infrastructure necessary to enable these software quality assurance and related activities.

b. The research infrastructure desired in response to this TTA will be a software assurance facility and the associated services that will be made available to both software analysis researchers and software developers, both open source and proprietary. Software analysis researchers will have access to services allowing them to test new algorithms for static, dynamic, and binary analysis against a variety of software in a multi-platform environment. Software developers will gain maximum value through access and use of many software analysis tools, including those funded by DHS S&T, open source analysis tools, and potentially commercial tools, without having to acquire licenses or learn how to use each one individually. DHS expects the SWAMP to become a national level resource in software assurance for open security technologies, used across civilian agencies and their communities as both a research platform and core component supporting US Government supported software development activities.

c. The resulting software management infrastructure will enable: (1) research into new forms of software analysis and testing, (2) analyses to run in reliable and repeatable workflows, (3) on-demand access to extendable computing resources, e.g., high performance computing clusters), (4) expansion to new forms of analysis and testing, such as dynamic analysis, and (5) tool isolation. Additionally, DHS S&T anticipates commercial vendors will be incentivized to participate through procedures that provide useful feedback to their ongoing development and refinement work without violating intellectual property and competitive business practices.

d. The main activities in building and providing the research infrastructure in response to this TTA are:

(1) Providing a core cyber infrastructure system in the form of combined hardware and software capable of testing multiple software packages in parallel using multiple software vulnerability analysis tools across multiple and varied platforms. Multi-platform capability is a requirement.

(2) Integrating the core system with available input processes (i.e. analysis tools and source code packages as the objects of analysis) and available normalized output functions to create an overall workload management and execution system exposed as a web-based accessible service to developers and maintainers of open source and potentially others.

(3) Managing the integrated system as a service, coordinating its functions with DHS S&T's HOST initiative (see below), and maintaining and enhancing the services provided to meet evolving customer requirements. An Initial Operating capability (IOC) for this system is expected within 15 months of the start of activities.

(4) A simple functional diagram representing the system is shown in Figure 1 below.

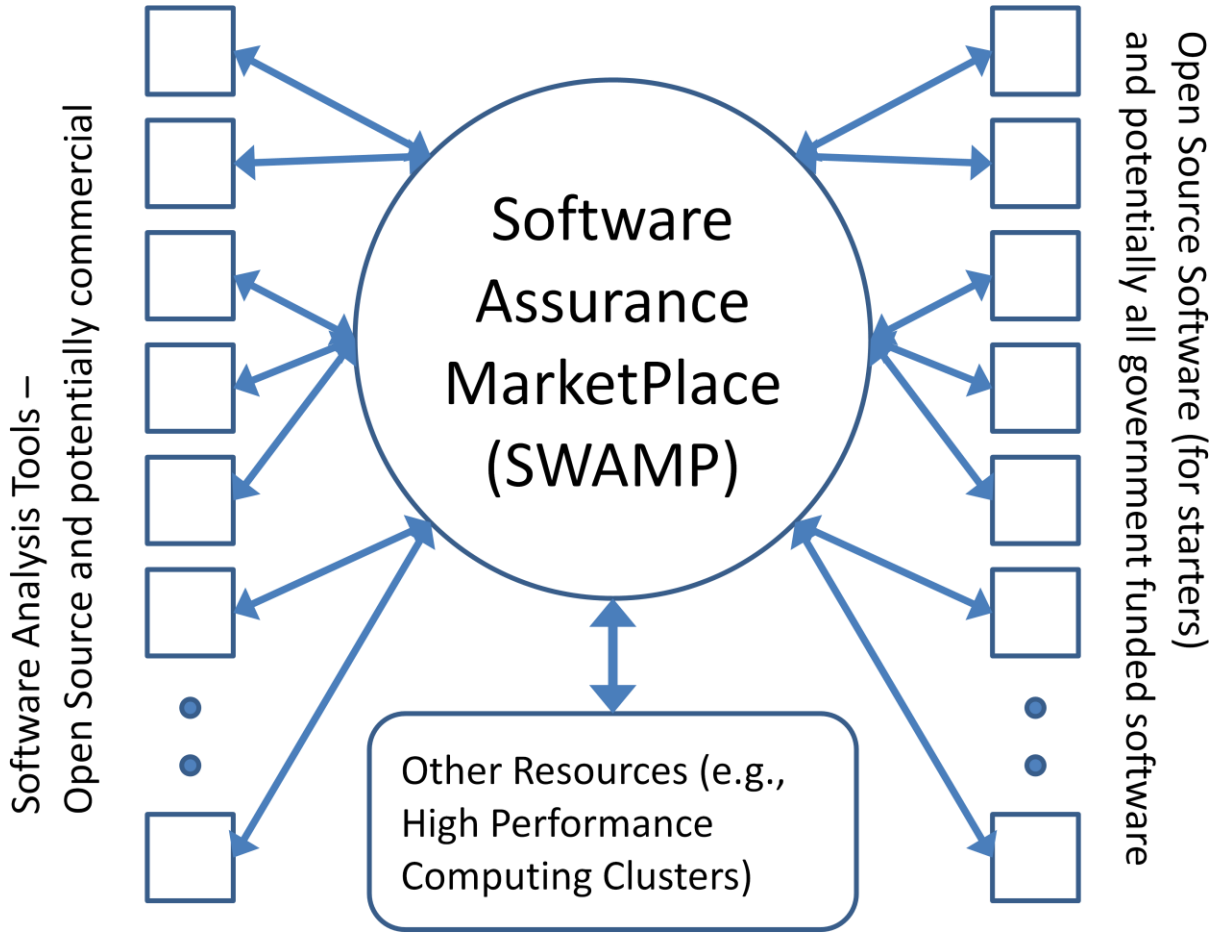

Figure 1. SWAMP Conceptual Architecture

e. This TTA is a special topic and falls outside of the Type I-II-III structure for proposals described elsewhere that applies to all other TTAs. The following proposal guidance, unique to this TTA, is provided:

(1) Proposals should not address development of new software analysis tools (see TTA#1), and instead should focus on leveraging existing software analysis tools which are themselves available in open source as part of an initial operating capability (IOC) with plans for subsequent technical support for integrating commercial analysis tools as coordinated by and provided through DHS.

(2) Performers can expect guidance from DHS on a set of open source code packages to successfully run through the system as part of the IOC. An IOC should be scheduled for no more than 15 months after the start of project activities. The proposal should describe the IOC and proposed metrics associated with the milestone. Performers should expect IOC to be a minimum of 5 software analysis tools and 100 open source software packages.

(3) Teaming is strongly encouraged, though not required. DHS reserves the option to make a single comprehensive award covering all aspects of SWAMP, or to execute a set of contracts covering required functions, depending on the scope and potential impact of proposals received. Proposals may address a single component if desired, but proposals must describe how they would interface with the entire SWAMP system.

(4) Proposals should address access to computing resources, especially when considering scaling and performance of the system in usage scenarios involving multiple and simultaneous users testing multiple source code packages in a multi-platform environment. Proposals may wish to consider a long term strategy involving access to high performance computing facilities.

(5) Proposals are encouraged to leverage standards, reference material, and functional capabilities that already exist or are under active development, where appropriate. Examples may include: the Software Assurance Findings Expressions Schema (SAFES), the Common Weakness Enumeration (CWE), the Common Vulnerability Enumeration (CVE), the Common Attack Pattern Enumeration and Classification (CAPEC) and related canonical and standards efforts supported by DHS National Cyber Security Division's (NCSD) Software Assurance Program (see https://buildsecurityin.us-cert.gov/swa/index.html); NIST's National Vulnerability Database (NVD), Security Content Automation Protocol (SCAP) and National Software Reference Library (NSRL); and the Tool Output Integration Framework (TOIF) and other Phase II 9.2 SBIR activities currently funded by this program (see http://www.cyber.st.dhs.gov/sbir9.2 for additional information).

(6) Proposals describing new approaches, methods and creation of new infrastructure, in cases where alternatives already exist, are expected to discuss the merits and advantages of their new research and development in comparison.

(7) Proposals should address security issues, challenges, and risk mitigation plans for the proposed system itself. This may include authentication and authorization approaches, system security, and physical security of the facility.

(8) Proposals may assume the following funding profile: up to $5M in Year 1; up to $5M in Year 2; and option years for up to three additional years at undetermined limits. These limits are the maximum expected funding values for the TTA.

(9) As a research topic, proposals are expected to advance the state-of-the-art in software assurance. Therefore, while establishing research infrastructure is a goal of this TTA, proposals are expected to include research activities as part of the infrastructure development and integration activities.

(10) As with TTA#1, the program seeks to couple activities funded in this TTA with a new effort called "Homeland Open Security Technology (HOST)", whose goal is to facilitate Government-wide secure IT solutions based on open source technologies. HOST will enable more effective access to vetted open source and related technologies used within the Government. One goal is to include in this initiative a process of rigorous test and evaluation of software in source and binary form relying heavily on automated processes. More information on HOST can be found at http://www.cyber.st.dhs.gov. Proposals in this TTA are encouraged to consider how their activities will integrate with the HOST program.

APPENDIX B
APPLICABLE PROVISIONS AND CLAUSES

FAR 52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address:

http://farsite.hill.af.mil/vffara.htm

NUMBER	TITLE	DATE
52.209-2	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS-REPRESENTATION	JUL 2009

FAR 52.252-2 Clauses Incorporated by Reference (Feb 1998)
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address:

http://farsite.hill.af.mil/vffara.htm

NUMBER	TITLE	DATE
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	JAN 2009
52.227-14	RIGHTS IN DATA – GENERAL	DEC 2007
52-227-17	RIGHTS IN DATA – SPECIAL WORKS	DEC 2007

Appendix C - List of Acronyms and Abbreviations

AIS	Artificial Immune System
BAA	Broad Agency Announcement
BGP	Border Gateway Protocol
BIS	Biological Immune System
CA	Cooperative Agreement
C.A.D.	Contract Award Date
CAPEC	Common Attack Pattern Enumeration and Classification
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CCR	Central Contractor Registry
CFDA	Catalog of Federal Domestic Assistance
CNCI	Comprehensive National Cybersecurity Initiative
COB	Close of Business
COTR	Contracting Officer Technical Representative
CSD	Cyber Security Division
CSIR	Cyber Security Incident Response
CV	Curriculum Vitae
CVE	Common Vulnerability Enumeration
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DETER	Cyber Defense Technology Experimental Research
DHS	Department of Homeland Security
DKIM	Domain Keys Identified Mail
DNS	Domain Name ~~Server~~ System
DNSSEC	Domain Name System Security
ELM	Enterprise-level Security Metrics
EST	Eastern Standard Time
FAR	Federal Acquisition Regulations
FedBizOpps	Federal Business Opportunities (www.FedBizOpps.gov)
FFRDC	Federally Funded Research and Development Centers
GAO	General Accounting Office
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFS	Government Furnished Services
GFR	Government Funded Resources
HBCU	Historically Black Colleges and Universities
HOST	Homeland Open Security Technology

HSARPA	Homeland Security Advanced Research Projects Agency
HUBZone	Historically Underutilized Business Zone
I3P	Information Institute for Infrastructure Protection
IEEE	Institute of Electrical and Electronics Engineers
IOC	Initial Operating Capability
IP	Internet Protocol
IR&D	Independent Research and Development
ISP	Internet Service Providers
IT	Information Technology
MB	Megabyte
MI	Minority Institutions
MTD	Moving Target Defense
NAICS	North American Industry Classification System
NCLY	National Cyber Leap Year
NCSD	National Cyber Security Division